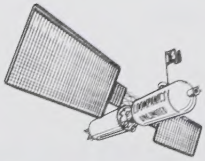
Modern Frauds and Con Games

BY TONY LESCE

Modern Frauds
and
Con Games

by Tony Lesce



Loompanics Unlimited
Port Townsend, Washington

Neither the author nor the publisher assumes any responsibility for the use or misuse of information contained in this book. It is sold for entertainment purposes only. Be warned!

Modern Frauds and Con Games

Published by:
Loompanics Unlimited
PO Box 1197
Port Townsend, WA 98368

Loompanics Unlimited is a division of Loompanics Enterprises, Inc.
Phone: 360-385-2230
Fax: 360-385-7785
E-mail: service@loompanics.com
Web site: www.loompanics.com

Cover by Craig Howell

ISBN 1-55950-224-x
Library of Congress Card Catalog Number 2002100650

Contents

Introduction

The dawn of the new century has seen an explosion in fraud for several reasons. Perhaps the most important reason is that new technology, such as the Internet, has expanded the horizons for fraud perpetrators. The Internet allows remote control frauds because the fraud artist can be literally thousands of miles from his victims. The proliferation of telephone service and telemarketing has also promoted fraud. The cost to the telecommunications industry alone is about $4 billion per year, and the cost to consumers is much higher. Today, you can order goods by telephone with a credit card, and anyone who steals or duplicates your cards can order a lot of merchandise in your name. "Pay at the pump" with a credit card is a welcome timesaver, but makes it easy for a fraud artist because all he has to do is swipe the card through the card reader, without signing a slip or entering a PIN number. The anonymity works in favor of the fraud artist.

Another reason is that some criminals are becoming smarter. The more perceptive ones realize that nonviolent crime is more profitable and carries less risk than violent crime. A low-grade stick-up artist collects perhaps $50 from a gas station or convenience store and risks at least five years behind bars. A bank robber can steal only a few thousand dollars in most cases, but a bank robber takes an appalling risk as well. From the moment he enters the bank, he's on closed-circuit TV, and his image is recorded. Law enforcement officials make great efforts to apprehend bank robbers, especially if they harm anyone during the course of a robbery. Finally, the penalties are much more severe, partly because we punish violent crimes more heavily and partly because it's possible to bring an array of charges against a robber. By contrast, the fraud artist consummates his crimes at a distance, greatly reducing the risk of identification and apprehension. With imagination, a fraud artist can do very well for himself, especially if he makes good use of modern technology such as the Internet.

Louis Freeh, former Director of the Federal Bureau of Investigation, warned in November 1999, that the computer and the Internet have allowed criminals to outmaneuver law enforcement because of the remote access they provide.[1]

During the latter part of the 20th century, there was a study measuring the intelligence quotients of prison inmates. It turned out that the average IQ was 85, and this led some people to believe that criminals tended to be dull-witted thugs. Actually, 85 was the

average IQ of criminals who had been apprehended, prosecuted, and convicted, not criminals as a whole. Obviously, many of the smarter ones remained at large. There's no reason for believing that criminals are any more stupid than the general population. Successful criminals who run "crime families" or who practice profitable con games tend to be above average in intelligence. If they weren't, they'd be behind bars.

Another reason for the proliferation of fraud is that our law enforcement establishment is set up in a manner that is obsolete, concentrating on local crimes and crimes of violence. In the United States, more than in many other countries, law enforcement is fragmented, with literally thousands of agencies policing their limited jurisdictions. The few federal agencies are limited to enforcing a small array of crimes, such as counterfeiting and the espionage statutes. The multiplicity of agencies leads to duplication of efforts, such as the federal Drug Enforcement Administration, state police, county sheriff, and local police all enforcing the drug laws. Despite the occasional "area drug task force," most efforts are not coordinated.

Fraud artists take advantage of this weakness. They make use of mobility to stay a step or two ahead of the law. We'll see examples of this again and again as we discuss different types of frauds, because people, including criminals, are more mobile today than ever before in history. People travel from one city to another, and one country to another, using many different forms of transportation. Fraud artists have a special incentive to relocate regularly, and the recent

downturn in air travel resulting from the September 11, 2001, terrorist attacks is unlikely to cramp the mobility of scammers.

The Postal Inspection Service is barely making a dent in the use of the mails for fraud. Instead, the Service seems to concentrate its efforts on prosecuting people who buy child pornography, who are vulnerable because they're not savvy career criminals who know how to evade detection. Surveying the U.S. Postal Inspection Service's Web site[2] showed that child pornography takes up much more space than fraud. For example, the Postal Inspection Service lists news articles, and for the month of August 2001, of the 40 articles listed, 30 dealt with child porn. The list of 22 wanted persons published on the Postal Inspectors' Web site shows only one wanted for "mailing of obscene material." Postal Inspectors are more adept in catching porn purveyors than fraud artists, apparently. This is probably because child porn is a "hot button" crime, and people get more excited about crimes against children than they do about crimes against property, such as fraud. Another reason is that people who buy kiddie porn are not hardened, street-smart professional criminals, and are not adept in avoiding apprehension.

FBI figures show that "white collar crime," another name for fraud, is a $500 billion industry in the United States. Each year, fraud artists steal that amount, and the number is constantly going up, especially because the FBI's figures are necessarily in-

complete. Another estimate is $750 billion from identity theft alone.

Fraud is the highest growth industry in the world, which is why it's become a global trillion-dollar problem. One reason is that it's low-risk compared to other crimes. Overall, the apprehension rate is about three percent and the conviction rate is about one percent.[3] By contrast, the apprehension rate for murder is about 67 percent, and for burglary between 13 and 15 percent, according to FBI figures. This is why criminals are turning to fraud as the wave of the future.

Contributing to the low apprehension rates for various types of frauds are the scammers' methods of operation. Those conducting outright, illegal frauds tend to be fast movers. They rely on distance and mobility to evade detection and subsequent prosecution. Fraud artists operate across state lines, and even across national boundaries. Telescammers set up a "boiler room" (a rented office with rented desks and banks of telephones), and a few weeks later are working in another state or country, thereby keeping a few jumps ahead of the law. As a rule, if you don't detect the fraud within three or four months, recovering the costs is practically impossible.[4]

As scammers gained the insight that distance and mobility are the keys to avoiding apprehension, they refined their techniques to create distance between themselves and their victims, and to avoid being pinned down in one spot. The "rip and tear" technique is the extreme form. This involves conducting telescamming from multiple locations, such as pay phones, hotels, etc., and changing locations daily.

Collecting the money also involves safeguards for the scammers. Instead of accepting checks or credit cards, they have their victims send money orders to a mail drop, or wire them the funds by wire transfer, such as Western Union. They also employ couriers to make the pick-ups, because the couriers cannot be directly connected to them. In some instances, they even conduct countersurveillance, to discover if their pick-up points are under surveillance by law enforcement officers.

As we'll see, law enforcement agencies are mostly living in the past, organized to cope with crime patterns of the last century. Victims have limited recourse because fraud artists are so remote, so hard to trace, and so mobile. And public education has not alerted people to the scope of the problem.

We don't even know the full extent of the problem, partly because of under reporting, and partly because of deficient record keeping. There is no central reporting bureau devoted to fraud statistics and analysis. Even if there were, the evidence shows it would not present a complete picture because many crimes are under reported. The Department of Justice's National Victimization Survey shows that a significant percentage of street crimes are under reported, even serious ones. For example, only about half the rapes in this country come to the attention of the police.

Non-violent crimes are reported even less frequently, for various reasons. Employers who discover employees stealing from them typically do not prosecute because it takes up their valuable time, and they

don't want to spend many unproductive hours in a courtroom. Banks and insurance companies, especially, have great concern over their reputations, and want to avoid any publicity that might suggest that customers' money isn't safe with them. Many employers will seek restitution, and terminate the offender, but that's as far as it goes. This reluctance to prosecute enables the embezzler to seek employment elsewhere and resume operations. Aggravating the problem is the reluctance of prosecutors to accept cases under a fixed dollar limit. Their resources are already stretched, and they don't want to clog up their systems with many small cases that cost more to prosecute than the dollar amount stolen.

There's another reason as well. Many fraud victims are ashamed to admit that they've been suckers for a scam. It's always a shock for victims to discover that they've been outwitted, and many fraud victims are afraid to step forward for fear of what other people will think of them. This reluctance to report fraud simply makes it easier for the scammers, because it keeps law enforcement officials unaware of how serious the problem truly is.

My previous book, *21st Century Fraud,* described many scams, but new ones cropped up from the moment the book appeared in print. The simple fact is that new and menacing techniques of fraud spring up almost every day.

This volume describes other methods of fraud, many of which are not even illegal, but do involve deception for economic gain. Published studies of the effectiveness and safety of new pharmaceuticals are an excel-

lent case because drug companies have a vested interest in selling their products to the public, and people can be hurt by using ineffective or unsafe drugs. The rash of recent lawsuits concerned with pharmaceuticals shows this clearly.

Fraud isn't necessarily perpetrated by stereotypical organized crime figures with ethnic sounding names. As we'll see, many "respectable" companies use deceptive practices, and many have been convicted of defrauding the government and consumers. These racketeers include people we tend to respect and trust, such as doctors and dentists.

Legitimate companies are often accessories to fraud. The telephone company, for example, rents lines to everyone, regardless of honesty, based only on their ability to pay. The telephone company's security department concerns itself only with persons who try to rip off the telephone company, not those who use its lines to defraud other people. Indeed, fraud artists have long-distance contracts with various telephone companies to support their boiler room operations, and the telephone service providers earn a lot of money catering to criminals.

Likewise the credit card providers. They recklessly send out "pre-approved" applications to everyone on their mailing lists, aware that some fraud artists raid mailboxes to snag those unsolicited applications and use them fraudulently. Granted, they'll lose some money to fraud artists, but consider that simply as the cost of doing business. They increase their interest

rates to cover their loses, making the consumer pay for it in the end.

There are, however, two basic human reasons why fraud prospers. One is greed. Some people are incredibly greedy, incredibly eager to "get rich quick," to an extent that overpowers their critical judgment. They hear what they want to hear, and thereby fall victim to a canny fraud artist.

The other reason is diametrically opposite: altruism. Many people are kind and generous, and thereby are potential targets for fraudulent charity scammers. It's important to note that both legitimate charities and outright frauds take advantage of people's altruism. Both exploit the kindness of people to take in billions of dollars a year. The legitimate charities at least pass on some of the money they collect to the people they're purporting to help, although in many cases their "operating expenses" appear suspiciously high. The fake charities keep it all.

How to Use This Book

Read this volume chapter by chapter, in sequence. The reason is that the earlier chapters lay the groundwork for later ones. There is also some overlap between chapters because fraud artists use different tactics for the same ends. For example, credit card scammers use the telephone, the U.S. mail, and the Internet to run their frauds. Some will begin by picking the victim's pocket. Identity theft is a component of various other scams and rackets. One of the last

chapters, "Protecting Yourself," discusses how to defend yourself against various scams explained in earlier chapters. This is the largest chapter in the book because this is a practical book, not an abstruse academic study. This chapter lays out steps you can take to reduce your vulnerability to fraud, and it's full of practical information you can use.

If your reading time is limited, and you feel you won't be able to get through this book within the next week or two, read "Protecting Yourself" first, and begin to follow the steps outlined in the chapter. The value of most precautions outlined will be self-evident, and you'll begin to get immediate benefit from this book.

No book on fraud can be the final word. This is why the last chapter is a list of resources you can use to obtain up-to-date information on various new types of frauds. There are new wrinkles appearing literally every day, and it's important to be aware of some of them.

You can't know them all. However, if you're in a situation in which you think you might become the victim of a fraud, look it up in one of the Internet sources listed. This will get you a quicker answer than contacting your local law enforcement agency.

Notes

1. Brunnstrom, David, "Computer Crime Outrunning Law Enforcement," Reuters, November 8, 1999, *ZD Net News*.

2. www.usps.gov/websites/depart/inspect
3. Global Fraud Alert, www.globalfraudalert.com
4. Daniels, Dave, Certified Communications Security Professional, *Credit Card and Identity Fraud Scams*, p. 6.

Chapter One
Medical Fraud

Doctors have a long tradition of shady practices, dating from the dark ages of medicine that ended only during the 19th century. Before then, there was practically no science in medicine, and doctors were little better than faith healers. Unscrupulous doctors ruthlessly exploited their patients' ignorance to extract higher fees, or to pretend to be treating them when they knew that no effective treatment existed.

Quacks and Ineffective Treatments

During the 19th and 20th centuries, the line between a legitimate medical practitioner and a quack became much clearer than before. It became much easier to distinguish between a doctor who employed well-researched and effective therapies and one who used off-the-cuff techniques and devices that had never proven themselves in controlled studies. Nevertheless, quackery has not relented, and now that we're begin-

ning the 21st century there appear to be as many quacks as ever.

Various types of devices sold by people claiming that they have medical value are also with us. These include magnetic beds, cushions, and other devices using magnetism or electricity to work. A device called the "Stimulator" and another called the "Xtender" became the subjects of a federal court ruling.

The U.S. District Court for the Northern District of Ohio ordered the maker and distributor of these two devices to refund money to purchasers because these devices were sold in violation of the Federal Food, Drug, and Cosmetic Act. These electrical devices were advertised as effective for pain relief in migraine headaches, swollen joints, allergies, and other conditions. TV and newspaper ads featured celebrities touting the products, according to the Better Business Bureau.[1]

Medical frauds proliferated during the 20th century, and have not slackened during the new century. Some of the frauds included "kickbacks," fees paid to family doctors by specialists for referrals. Also included was "ghost surgery," with the surgeon leaving the operating room once the patient was anesthetized and having a lower-paid intern or resident perform the surgery. Billing patients for unnecessary treatments was another way of enhancing a crooked doctor's income.

With the advent of HMOs and state-sponsored medical care, new avenues of cheating opened up for the avaricious practitioner. Previously, a doctor could go only so far, because the patient paid his own bills

and would question some charges. With "third-party payers," Medicare, Medicaid, and HMOs, the unscrupulous medico sends his bills to the government or the central office, where a clerk with no direct knowledge of the patient or the treatments employed makes out payment vouchers. This system opens the door to many more abuses than before.

Unnecessary Treatments

Doctors have often increased their incomes by performing unnecessary treatments and operations on people of all ages. When a patient comes to a doctor with a problem, he depends upon the doctor's expert knowledge to help him. The situation demands that he place his trust in his doctor, because the patient does not have the specialized knowledge to help himself. If the physician states that the patient needs a certain treatment, the patient is in no position to refuse.

Often, doctors pad their bills by performing unnecessary but low-risk surgery such as newborn circumcisions. Some, however, are into the big-dollar markets. U.S. Attorney Patrick Fitzgerald said that a Chicago doctor specializing in cardiology allegedly performed unnecessary procedures, including angioplasty, and that two patients died as a result of these unnecessary procedures. The doctor's license had been suspended by the Illinois Department of Professional Regulation. There were also charges against the company that had employed the doctor, including kick-

backs and medically unnecessary tests and hospital admissions, costing Medicare and other insurers over $5 million.[2]

In the past, medical and surgical treatment depended more on the patient's ability to pay than other factors. Rich patients received more attention, more treatments, and more surgery than did less affluent ones. Today, Medicare and Medicaid provide funds for the treatment of lower income groups and there is less of a gap between the amount of care received by rich and poor. However, this has brought new problems.

The "graying" of the population means that today there are many older people needing medical care, and government programs to provide care for senior citizens. One of the unintended consequences of widespread government health care programs is that fraud artists see them as cash cows to be milked. Even "legitimate" doctors and hospitals have been convicted of overbilling, double billing, and fraudulent billing. The temptation is irresistible for some when so much money is available.

Figures gathered by the Health Insurance Association of America show that fraudulent diagnosis comprises 43 percent of medical fraud cases. Billing for services not provided is the second largest category, with 34 percent of the cases.[3]

One such example was a Massachusetts registered nurse who made home visits to psychiatric patients covered by Medicare. At the hearing where she pleaded guilty, Assistant U.S. Attorney Gary Katzman informed the judge that the evidence demon-

strated that this nurse had falsified her nursing notes to justify payments for home visits she never made.[4]

One woman in her 90s was referred by her family doctor to an ophthalmologist for her vision problems. He said that she needed laser surgery to clear her cataracts. The cost is $750 for each eye, but he told her son that Medicare would pay 100 percent. Her vision did not improve after the laser treatments, and the son was left wondering if the specialist's main motivation had been his mother's eyesight or the $750 paid for about five minute's work.

Another doubtful area arrived when his mother was in the last couple of weeks of her life, and in a nursing care facility. The nursing facility was well-run, and the son never saw any evidence of inadequacy. He received a telephone call from a woman claiming to be a nurse referred to him by his mother's family doctor, and who told him that during the last days of her life, Medicare would pay for "hospice care," supplied by her company. She was unable to describe exactly why his mother needed this additional care, or what deficiencies in the nursing facility had prompted this call.

The clincher was that Medicare would pay 100 percent for this "hospice care," and the son gave the company the benefit of the doubt and signed on the dotted line. His mother died a couple of weeks later, and during that time he never saw any sign of a hospice care worker when he visited her.

There have been instances of abuses connected with hospice care. Seventy-seven hospitals in New York state refunded over $1.7 million to Medicaid after overbilling for the care of patients sent to them by

hospices between 1994 and 2001. The problem arose because terminal care is covered under state Medicaid, and when a hospice sends a patient to a hospital it must bill Medicaid and then pay the hospital. What happened was that both the hospices and the hospitals were billing Medicaid for the same patients.[5]

Medicare's Office of the Inspector General found that Medicare had paid out about $48.5 million in error for uncovered treatments, medically doubtful treatments, and medically unnecessary treatments in the first half of 1999. As usual, the reasons ranged from sloppy documentation to outright fraud.[6]

Convictions for medically unnecessary treatments are rare because it's often a matter of opinion whether a patient needs a certain treatment. However, a podiatrist in Indiana pled guilty and was sentenced to 68 months in prison for mail fraud and criminal contempt. The U.S. Attorney for the Southern District of Indiana stated that the investigation had turned up that the treatments billed to Medicare were not medically necessary. Another result was that the podiatrist would no longer be able to participate in Medicare and other federally funded programs.

Another recent federal case involved a company that settled with the Department of Justice for $7 million, because many of the claims for payment were inadequately supported by documentation and not medically necessary. Claims accompanied by paperwork stating that the treatments were ordered by the patients' doctors were either inadequate or faked. These involved claims to Medicare, Medicaid, and TRICARE,

the military program covering health care. Significantly the case came to the government's attention because of a former employee who blew the whistle on his former employer in 1997.

"Operation Tooth Decay" in Florida resulted in the arrests of 18 people in August 2001. These individuals had been employed by dentists to "recruit" children and to drive them to the offices of participating dentists who then treated them for dental problems or even billed Medicaid for non-existent treatments. These drivers had earned between $2,000 and $50,000 each during the period of investigation, stated Florida Attorney General Bob Butterworth. The continuing investigation has resulted in 102 people arrested so far, including 15 dentists who were part of the racket.[7]

Another case involved Liberty Medical Supply and Liberty Home Pharmacy, in Florida. FBI agents searched for evidence and copied records, carrying out an investigation begun by the U.S. Attorney's Office for Southern Florida. The business publication *Barron's*, reporting on the case, stated that there had been allegations that the company shipped products that had not been ordered, or shipped products to people it knew were dead.[8]

Kickbacks

Kickbacks are still with us, but today they're better organized. A Kansas hospital and two doctors were convicted in April 1999 of accepting bribes for refer-

ring patients to a hospital. The hospital's CEO was also convicted, and the convictions were upheld by a three-judge panel of the federal appeals court in Colorado in 2001. The payments came to almost $1.8 million, disguised as consulting fees. The hospital had received almost $40 million for these patients' care from federal Medicare.

At times, the federal government investigates payments made to physicians. In one case, B.J. Carlen, formerly known as Pastor Medical Associates, agreed to pay $230,000 reimbursement for alleged improper Medicare billing. Pastor had an on-site laboratory to perform blood chemistry and other tests at the direction of Pastor physicians. According to the U.S. Attorney, the amount these doctors received annually was linked to the amount of business they referred to the lab.[9]

Another type of kickback relates to donated organs. An emergency room physician with a private relationship with a group that deals in organ transplants may be tempted to pronounce an accident victim dead if he knows he'll collect a finder's fee for his organs. In a state where consent to harvest organs can be on the driver's license, an unethical physician has a head start, compared to states where it's necessary to obtain consent from the family.

Live human tissue also commands a price. Most parents who consent to have their newborn sons circumcised are unaware that the foreskins removed during newborn circumcisions are sold to biomedical

companies that use them to grow artificial tissue used in the treatment of burns.

Double Billing

Florida Attorney General Bob Butterworth stated that one of the nation's most prominent HMOs would refund almost $8 million in duplicate billing because the health care group had billed both Medicare and Medicaid for the same care for the same patients. Butterworth said that an investigation into the entire industry was underway because more HMOs may have been involved.[10]

Duplicate billing errors occur, and proving that they are intentional is very difficult. Duplicate billing involves millions of dollars lost by federal and state health care agencies. One audit of Medicare found that over $2 million went out in duplicate payments in 1998. This audit was limited to only 15 "procedure codes," numbers used to denote specific medical care procedures, and the government hasn't got a handle on how much Medicare funds went for duplicate payments.[11]

One reason billing errors are so common is that Medicare billing is so complex, with code numbers denoting each type of diagnosis and treatment, and the level of treatment provided. Some health care providers use only high-level codes for some procedures, which means that they get paid for the most extensive and expensive treatment available. This "mono-coding" is a red flag for auditors who monitor Medicare

payments, because they know that medical conditions do not all require the same level of care.[12]

Non-covered Services

Medicare doesn't pay for everything, and some of the exclusions are chiropractic care and faith healing. However, one Virginia chiropractor got around this by enlisting medical doctors to perform initial patient examinations, then billing for chiropractic services under their names and provider numbers. This was to hide chiropractic services under regular patient billing, according to the U.S. Attorney for the Eastern District of Virginia.[13]

Some laboratories are providing "unestablished" medical tests, which are not covered under Medicare. These tests may be simply invalid, or experimental, and they do not conform to the Clinical Laboratories Improvement Amendments of 1988 (CLIA), according to the Office of the Inspector General. Nevertheless, some laboratories bill Medicare for these tests, knowing that they're likely to slip through the cracks.[14]

Counterfeit Drugs

Seniors consume pharmaceuticals more than younger people, and the high cost of pharmaceuticals has had a disproportionate effect on the older population. In the American Southwest, elderly people make regular trips to Mexico because they know that

they can buy drugs more cheaply south of the border. There is also a counterfeit drug industry that is very harmful to people, young or old.

This counterfeit drug industry operates on both sides of the border. Between five and eight percent of pharmaceuticals in the world today are counterfeit, according to one estimate.[15]

A complication of the counterfeit drug industry is that legitimate manufacturers can get sued for harmful effects of counterfeits. Even worse for the consumer is that the producers of bogus drugs are hard to locate and sue for damages.

Aggravating the problem is that Internet sites now sell drugs, and some of these are counterfeit. As we'll see in the section on Internet fraud, the anonymity of the Internet allows fraud artists tremendous latitude.

A classic motion picture that dealt with adulterated drugs on the medical market was *The Third Man*. Orson Welles played the part of a trafficker who sold diluted penicillin in post-World-War-Two Austria. Although this fact-based film dates from the immediate post-war era, this sort of trade still goes on today. One Latin American doctor recently spoke out about the problem of low-quality pharmaceuticals sold by unlicensed vendors. According to Dr. Ra Dul Duriz, of the Caracas, Venezuela Centro Medico, many peasants cannot afford conventional medical care, and treat themselves with antibiotics and other drugs bought from roadside vendors. These drugs are often diluted, expired, or faked, and one severe effect is that diluted or expired antibiotics lead to antibiotic

resistance by encouraging strains of antibiotic-resistant bacteria.[16]

By contrast, antibiotic resistance in industrialized countries is the result of over-use or inappropriate use of antibiotics. However, even the United States has a problem with counterfeit drugs. According to the World Health Organization, between five and eight percent of bulk drugs, from which tablets and capsules are made, imported into the United States are counterfeit.[17]

Counterfeit drugs are typically bulk drugs without proper documentation to show date of manufacture, storage conditions, quality control test results, and manufacturing procedures. In essence, they have no history, and could have come from anywhere. They may be outdated, ineffective, contaminated, or even outright fakes, because their provenance cannot be proved. A generic epilepsy drug made from bulk drugs that were not FDA-inspected led to deaths in 1996. Another drug, an antibiotic, imported in bulk and not adequately inspected, has been associated with 155 deaths.[18]

In January 2001, a counterfeit version of the AIDS drug Serostim appeared on the market. This carried the lot number MNH605A. Two other counterfeit drugs that appeared in 2001 were hormone replacements. One batch of counterfeit Neupogen had the lot numbers P000948 and P000890. Counterfeit batches of Nutropin had the lot numbers L9101A4, L9504A2, and L9404A3.[19]

Drug dilution is still with us, though. A Kansas City pharmacist surrendered to the FBI after an investigation revealed that some of the intravenous chemotherapy drug bags he provided contained greatly diluted amounts of the drugs prescribed. As drugs used for chemotherapy are very expensive, there is great profit in dispensing diluted doses. Tests run on some samples of drugs dispensed showed that the doses were between 17 and 39 percent of the strengths ordered by the doctors who prescribed them. Other reports stated that the concentration of the drug was as little as one percent. One FBI spokeswoman stated that at the dilution used, the pharmacy would have saved about $780 on one order of drugs.[20]

Diluting drugs is not only a financial loss to those cheated. Not only is the diluted medication less effective than the full-strength version, but the doctor treating the patient may decide that an increased dose is necessary. If the next treatment is with the full-strength drug the side effects can be severe and dangerous. Another effect can be developing a drug-resistant strain of the cancer cells.[21]

Fraudulent Health Products

There have been quack products promoted for centuries, mainly because years ago medicine was primitive and there was little to choose between a quack and a doctor of medicine. Today, the dividing line is much clearer, and there are categories of health-care-

related products that are clearly frauds. The reason quackery still exists is that there are many loopholes in our laws, and entire industries prey on the sick, under the guise of "alternative medicine." This is not to say that all forms of alternative medicine are bogus. Some are genuinely helpful, but the counterfeit ones hide in the shadow of alternative medicine. An example is herbal medicine.

Herbal products take advantage of the loophole in the law regulating pharmaceuticals and are sold as "dietary supplements" to avoid quality control regulations. Worse, much of the information about herbals is unreliable or misleading, as published information is not controlled by any law or regulation.

Many legitimate pharmaceuticals originated as herbal remedies, and legitimate drug companies spend a lot of resources examining herbal remedies to find those that have genuine medical value. The problems with herbal medicines sold in health food stores are several:

- Remedies that work for one condition being hyped as useful for many others as well.
- Herbal remedies manufactured with poor quality standards or no standards at all. Legitimate pharmaceuticals are made to exacting standards of strength and purity set up by the U.S. Food and Drug Administration. Herbals often are not, and vary greatly in strength and purity.[22]

  An analysis of several brands of St. John's Wort found that capsules varied in strength by a factor of 17. Another study found that 75 percent of the

capsules contained between 75 percent and 135 percent of the labeled strength.

- Totally useless herbals sold under the pretext that they cure or alleviate some conditions.

Herbals are not the only types of unreliable remedies. Many others are on the market, reaching credulous and vulnerable consumers through radio, television, and newspaper ads. Others advertise in magazines. Yet others are sold on the Internet, where outrageous claims can be made with little fear of consequences. The Internet is a popular vehicle of fraud because it's literally worldwide. A product or treatment advertised on the Internet by a Web site in another country may be sold by a local distributor, and when complaints result, the local office closes up and moves elsewhere, sometimes overnight.

What is the harm done by spurious health products? There are several harmful effects. The first is ineffectiveness for the condition to be treated. The consumer who self-medicates does not receive proper treatment for his condition.

Another and very obvious effect is the money wasted on fake cures. People with fatal diseases will give up their money before they give up their hope.

Finally, there may be harmful effects. Some people believe that herbal cures and other spurious devices have no side effects. This simply isn't true. Today, many doctors ask their patients if they're taking any drugs, herbals, vitamins, or other substances because they do have side effects. They can also interact with prescription drugs to produce unwanted effects. Antioxidant vitamins, for example, can nullify the effects

of drugs prescribed to fight high cholesterol. Large doses of Vitamin C can degrade the effect of local anesthesia.

Prescription Drug Hypes

One of the dirty little secrets of the pharmaceutical industry is that it spends more, much more, on promoting its products than on developing them. Drug companies employ public relations experts to plant stories in the media that the cost of drugs is so high because of the tremendous expenses involved in research and development of new products. Actually, advertising expenses exceed the research budgets. Worse, part of the research budget is devoted to financing medical studies to "prove" the effectiveness and safety of new pharmaceuticals. Most people don't know that the testing of new drugs is in the hands of the companies that develop them, not the U.S. Food and Drug Administration. This leads to a peculiar situation, not necessarily in the best interests of patients.

Pharmaceutical companies pay out research grants to doctors to test their new drugs as samples on patients. These doctors then publish their studies, and copies are handed to the FDA to secure approval of the new products. However, because pharmaceutical companies finance these grants, there is some question as to their validity and objectivity. What happens when research shows that a new drug doesn't work as planned? Does the study appear in medical journals,

or is it buried until another, more favorable study can be conducted? More to the point, how objective are the doctors who conduct such studies? With pharmaceutical companies paying for the research, how reliable can the research be?

For decades, we've seen a similar problem with "expert witnesses" hired by lawyers to plead their clients' cases in courts. Lawyers tend to hire an expert witness who will benefit their cases, not sink them. This is why expert witnesses have earned the name of "opinions for hire." Less polite terms are "hired guns" or "whores." Each lawyer has a stable of expert witnesses, from questioned document examiners to psychiatrists. At times, the bias is so obvious that it becomes ridiculous.

During the trial of John Hinckley, the man who shot and injured President Ronald Reagan, each side presented a panel of four psychiatrists. The prosecution wanted to show that Hinckley was legally sane and knew what he was doing, while the defense wanted to show that Hinckley was funny in the head, and not truly responsible for his actions. Not surprisingly, the four shrinks testifying for each side faithfully defended the interests of the party paying their fees, adjusting their testimony to suit their employers' needs.

When the question is whether or not a new experimental drug is both safe and effective, pharmaceutical companies naturally provide grants to doctors with a track record of coming up with positive results. A doctor who repeatedly finds that the experimental drugs

he tests are flops can't expect many grants in the future.

This is why studies paid for by pharmaceutical companies tend to present favorable results more often than those sponsored independently. This has led to a widespread concern among the editors of professional medical journals that studies paid for by drug companies might be biased. Frank Davidoff, Editor of the *Annals of Internal Medicine*, was quoted as saying, "It's become a huge problem."[23]

At times, the published study does not include the "methods" used to develop the data. Some companies withhold this, claiming it's "proprietary information." This leaves it up to the reader to wonder how the research was conducted, whether the sample size was adequate, whether selection of test subjects was biased, and how the tests were performed. There even have been charges that some drug companies withheld the results of research that was not favorable to their products.[24]

Pharmaceutical companies tend to hire professors at medical schools to conduct their research, as they are acknowledged experts in their fields and their opinions carry weight. However, even when a medical school tries to ensure objectivity by stipulating in grant agreements that the authors will be free to publish if the results are not what the company wants, there's still pressure to produce positive results, fueled by concern over getting research grants in the future.[25]

This is why medical journal editors adopted a policy of requiring the authors of pharmaceutical studies to back up the published studies. This requires the authors to vouch for the results of any study funded by pharmaceutical companies, and there is a uniform policy of refusing to publish questionable research papers.[26]

Another aspect of the problem has been pressure exerted on the Food and Drug Administration to "fast track" approval of new pharmaceuticals. This has had a deadly effect. Between 1997 and August 2001, there have been 12 prescription drugs taken off the market because of dangerous side effects. The latest was Baycol, a cholesterol-lowering drug withdrawn in August 2001, because there had been at least 31 deaths in the United States. There were more deaths in other countries.[27]

One heartburn prescription drug taken off the market, Propulsid, was the subject of a $1.2 billion lawsuit against its manufacturer, Janssen, and its parent company, Johnson & Johnson. The plaintiffs' attorney stated that the manufacturer changed the labels five times to prevent patients from learning adverse information about the drug. The plaintiffs stated that they suffered heart conditions, anxiety, and other symptoms while using the drug. The drug has been a factor in 80 deaths, and Janssen withdrew the drug in 2000. The jury awarded the 10 plaintiffs $100 million, and there are other lawsuits pending nationwide.[28]

Other medical products are also handled in a similar way. The U.S. Department of Justice stated that a former official of Micro Interventional Systems, Inc.

received a 10-month jail sentence for concealing and falsifying test results. Anna Maria Carillo allegedly made false submissions to the Food and Drug Administration to feign compliance with a requirement that these devices, including catheters, be tested for safety and effectiveness.[29]

Other Problems

Fraud is not the only hazard facing medical patients. Eli Lilly and Co., provider of pharmaceuticals, unintentionally revealed the e-mail addresses of over 600 people treated for several problems, including depression, who had subscribed to its Web site, www.prozac.com. According to a Lilly representative, this was the result of human error. This came about when Lilly sent an e-mail message to all subscribers advising them that they would be discontinuing its reminder service. Apparently the message contained a list of all addresses.

At a time when personal privacy is under attack, consumers should be wary of sharing any sort of personal information on the Internet. Let's look next at Internet fraud.

Notes

1. http://www.bbb.org/alerts/stimulatorII.asp
2. *Compliance Monitor*, Wednesday, October 17, 2001.

3. *Compliance Monitor*, Wednesday, September 19, 2001.
4. *Compliance Monitor*, Wednesday, October 3, 2001.
5. HCPro Complianceinfo.com.
6. *Compliance Monitor*, Wednesday, August 8, 2001.
7. *Ibid.*
8. *Compliance Monitor*, August 29, 2001.
9. *Ibid.*
10. HCPro Complianceinfo.com
11. *Ibid.*
12. *Compliance Monitor*, Wednesday, August 8, 2001.
13. HCPro Complianceinfo.com
14. *Compliance Monitor*, Wednesday, August 8, 2001.
15. "Drug Counterfeiting: A Bitter Pill," *Security Management*, Volume 45, Number 9, September 2001, p. 16.
16. "Counterfeit Drugs Lead to Antibiotic Resistance in Developing Countries," *Global Fraud Alert News*, September 25, 2000.
17. Twersky, Ori, "Counterfeit Drugs Creep Into U.S. Market," *WebMD*, Washington, DC, June 8, 2000.
18. *Ibid.*
19. *Ibid.*
20. Freed, Josh, Associated Press, "Man Accused in Drug Dilution," *Albuquerque Journal*, August 16, 2001, p. A9.
21. Fields, Dana, Associated Press, "Pharmacists Say Risks High if Cancer Drugs Are Diluted," *Albuquerque Journal*, August 17, 2001, p. A8.
22. Barrett, Stephen, M. D. "The Herbal Minefield," *Quackwatch*,

www.quackwatch.com/01QuackeryRelatedTopics/herbs/html

23. Okie, Susan, *Washington Post*, "Medical Editors Set Strict Policy," *Albuquerque Journal*, August 6, 2001, p. A6.
24. *Ibid.*
25. *Ibid.*
26. *Ibid.*
27. Neergaard, Lauran, Associated Press, "Baycol Yanked off Shelf," *Albuquerque Journal*, August 9, 2001, p. A1.
28. Bulkeley, Deborah, Associated Press, "Jury Awards $100 Million in Drug Case," *Albuquerque Journal*, September 29, 2001, p. A12.
29. *Compliance Monitor*, Wednesday, September 12, 2001.

Chapter Two
Internet Fraud

The Internet has brought a new rash of problems unique to this medium. The Internet is literally worldwide, and anyone with a computer wired into the Internet is free to post what he wishes. The Internet offers an unprecedented opportunity to propagate spurious information because it's difficult or impossible to verify the source.

Spurious Newsletters and Spam

Some scam artists produce fake online newsletters, purportedly designed for a special interest group or offering advice on everyday problems. Actually, these are thinly disguised advertisements. Typically, they contain headlines such as "How to Take Care of Your Headache" and a link to a Web site offering a product or service for sale. All of the "news" items discussed have links, and these are aimed at credulous people who can't recognize an ad if it bites them.

Unsolicited advertising e-mails, called *Spam*, also claim to help the reader with a problem, and they contain links to Web pages and Web sites that offer products or services for sale. Some of these are outright frauds, promising products or services that are never delivered.[1]

Other items are low-grade counterfeits or outright junk. Some of these fraud artists promote gemstones or rare coins as "investments." These items are often shipped in a sealed plastic container, and the seller warns the victim not to open the container because this would void the warranty of the items. This is just a trick to deter the victim from having the items appraised, which would reveal that the items were junk or fake.[2]

Another trick used by these scammers is "reloading." Once they realize they have some credulous suckers on the hook, they tell their victims that others are interested in purchasing the items, and advise them to buy yet more in order to realize a greater profit when they resell them. This is a straight appeal to the victim's greed. After the victim buys the additional quantity, the promised "buyer" evaporates, and the victim faces an even greater financial loss.[3]

Online Auction Frauds

Some online auctions are outright frauds. The Federal Trade Commission stated that last year brought a 20-fold increase in online auction fraud complaints. Not all people who advertise on the Net are honest.

One man who thought he was getting a good deal on a used car got burned. He sent his check in payment, but eight months later still had not seen his car. Barry Johnson, of Virginia Beach, admitted in court that he'd taken part in a phantom goods scam on the Net, putting non-existent items up for auction on E-Bay and Yahoo Auction Net. Johnson had gone to a parking lot and taken a picture of a silver Mercedes to send to the victim as proof that he had the exact model and color desired.[4]

There's another reason to be wary of Internet auctions. Even when the merchandise is real and the seller ships it to you upon receipt of your money, there's room for trickery, using the old tactic of employing shills. These people enter bids to drive up the price, and you end up paying more than you would have otherwise. Using shills on the Internet is easier than in a face-to-face auction, because the seller can enter bids using a variety of aliases to produce the impression that many people are bidding on the same item. This is a good reason for knowing exactly what you're buying, and what a fair price is.

Investment frauds are also proliferating over the Internet. Bogus news about overvalued stocks has stung many credulous investors, and other Internet investment scams are bogus offshore "prime notes" and pyramid scams. Fake news is the tool of "shills," people who purposely promote a stock, bond, or other product on message boards to persuade others to buy.

These messages are typically anonymous, the people "identifying" themselves with aliases or "handles" such as "Jack Sprat" when they post. This points up

the importance of the old dictum "Consider the source."

Some bogus investments are in precious metal or diamond mines in far-off countries. The seller never tells the investor, or victim, that the mines are undeveloped or inoperative, and the reason they're always in a remote location is to deter personal visits by victims.[5]

Yet another, and potentially more dangerous fraud, is the e-mail scam that asks you to provide your account numbers, credit card numbers, and expiration dates on some pretext. The latest wrinkle in this type of scam is disaster relief for the victims of the World Trade Center attacks, as we'll see in the chapters covering fake charities. No legitimate business or charity will ask you for this information unless you're buying something.

Internet Download Scams

If you download programs from the Internet, you may be buying trouble. This is a variant on the "809" scam, and uses entertainment programs as the lure. The program you download may be designed to disconnect you from your regular Internet Service Provider (ISP) and reconnect you to a provider in another country without your knowledge. Then you get hit with long-distance charges and even a per-minute charge from the other ISP.

This type of scam is particularly dangerous if you have children using your computer. They don't require

a credit card or other direct payment method, and some connect to music videos, games, and even porno sites.

Although the Internet provides some high-tech aids to fraud artists, scammers are still making good use of older technology, such as the telephone. Internet scams are passive, in the sense that they require the victim to log on to a Web site. The telephone permits fraud artists to aggressively seek out victims, using modern computerized telephone dialing techniques.

Notes

1. http://www.usdoj.gov/criminal/fraud/telemarketing/schemes.htm
2. *Ibid.*
3. *Ibid.*
4. McGlone, Tim, "Beach Man Admits Role in Scams on Net Bidders," *The Virginia-Pilot*, July 31, 2001, www.pilotonline.com
5. http://www.usdoj.gov/criminal/fraud/telemarketing/schemes.htm

Chapter Three
Telephone Scams

Today almost everyone has a telephone, and many people have more than one. The telephone makes it very convenient for a scam artist because it permits remote-control fraud. The scammer doesn't have to be within physical reach of his victims, or even in the same state. A remote-control fraud makes it more difficult to hold the scammer accountable. According to the National Fraud Information Center dishonest scammers bilk consumers of about $40 billion a year.[1]

The telephone also puts people within reach of a new menace, the "telemarketer." While salespeople have used the telephone for decades as a sales tool, today's telemarketing is much more sophisticated than the crude telephone selling of years ago. Wide Area Telephone Service (WATS) makes it economical to telephone people across state lines, and computers work to save the telemarketer time and make even more people accessible.

Telemarketing is like what Winston Churchill called "The Wizard War," a game of countermeasures and defensive tactics. In simpler days, paying an extra fee to have an unlisted number would make it very difficult for a telemarketer to reach the person with such a number. Today, a computer programmed for sequential dialing rings every possible combination of numbers in sequence, and it doesn't matter at all if the number is listed or unlisted.

Caller ID, in theory, allows you to know who's calling, but telemarketers have been successful in defeating it in several ways. First, telemarketers lobbied to have "blocked call" service, which does not display the caller or his number on the Caller ID. This was on the pretext that abused women telephoning their husbands from shelters did not want the husbands knowing where they were. Consumers with Caller ID quickly learned that when "Private Call" or "Blocked Call" displayed on their screens, it was likely a telemarketer. Telemarketers then adopted a new countermeasure, using PBX switchboards and other electronic trickery to make the display show "Out of Area."

Some people do not answer calls unless they can identify the caller, while others screen their calls with answering machines. To save time on fruitless dialings, telemarketers programmed their computers to dial several numbers at a time on different lines. The first one to answer gets the telemarketer's attention. The computer just hangs up on the others, and they

find themselves answering a dead line. This accounts for the profusion of "hang-up calls" today.

Many telemarketing efforts are more or less honest, in the sense that the callers are trying to sell a product or service that they actually deliver. However, many others are outright scams that are designed to defraud from the get-go.

Another indicator of the inherent dishonesty of telemarketers is that they tend to use aliases. Hardly any tell their real names when they call. This is true whether they're actually selling a product or service, or they're outright scammers. This merely goes along with their other deceptive tactics, such as masking their telephone numbers.

According to the National Fraud Information Center, fraudulent telemarketers have favorite states from which they operate. The top five are Arizona, California, Florida, New York, and Texas. There are also many fraudulent calls made from boiler rooms in Canada.

The telephone system makes it possible to victimize people from far away. This is a basic tactic of telephone-scam boiler rooms because it takes advantage of the fragmentation of American law enforcement. A telephone scammer who calls his victims from another state knows that if the victim files a complaint with local police, it will take time to establish liaison with law enforcement officials in the state where the scammer is currently operating. An additional complication is that the wording of anti-fraud statutes is different in different states, and prosecutors must get all their ducks in a row before they can act. By the time

law enforcement officials are ready to move, the fraud artist has pulled up stakes and established himself in another state.

Canada — A Special Case

This problem is even worse when the fraud artist operates across national boundaries, such as the border between the United States and Canada. Canada is divided into ten provinces, and its law enforcement structure is as fragmented as that of the United States.[2]

There are several federal agencies dealing with law enforcement, the best known of which is the Royal Canadian Mounted Police (RCMP), also known as the "Gendarmerie Royale du Canada" (GRC), in that bilingual country. The RCMP polices some provinces, such as Alberta and British Columbia, but other provinces have their own state police forces. Two examples are the Ontario Provincial Police (OPP), and the Surete de Quebec (SQ). Additionally, larger Canadian cities have their own police forces. Toronto is one, and Montreal is another. All of these police forces vary widely in professionalism, competence, and corruption.

For practical purposes, the Canadian and American telephone networks are one. It's as easy to make a telephone call from Tucson to Montreal as it is to Los Angeles, by dialing the appropriate area code. There is no "country code" as there is to reach a nation in Europe or Asia. This makes it very easy for the tele-

phone scammer. A fraud artist based in Canada can lose himself behind a screen of multi-agency barriers because it's even more difficult to prosecute across national boundaries than across state lines.[3]

According to the FBI, half of the telemarketing fraud complaints it receives are about con artists operating from Canada. There is a special reason for this, connected with law enforcement. Canadian authorities are less concerned about crimes committed against other countries than they are about crimes within Canada. Some of these crimes include fraudulent Canadian lottery scams and other more conventional telemarketing frauds.[4]

Added to this is the ease with which a criminal can establish residence in Canada. Canadian immigration is even more porous than the United States', and a criminal can come to live in Canada using several pretexts. Once in, he can assume a new identity. Canadian authorities will not pursue him vigorously.[5]

American authorities can ask for extradition from Canada. Given the traditionally friendly relations between the two countries, the Canadian Government will usually grant extradition. However, to extradite someone, it's necessary to locate him, and as we've seen, fraud artists are quick on their feet. In Canada, as in many other countries, a moving target is hard to hit.[6]

Recycling money is essential to many criminal operations, not only fraud. Canada is also a good place to launder money, because Canadian money laundering laws are weak and not well enforced.[7]

Victims

Although no age group is immune, most of the telephone scams victimize people over 60. One obvious reason for this is that older people tend to be at home more than younger groups, who go out to work every day. There are, however, other opinions regarding why older people seem to be favorite targets. Some say it's because older people are more trusting. Others say it's because fraud artists believe older people have more money.[8]

Statistics gathered by the National Fraud Information Center show that, although some fraud operators use other means of making contact, such as mail advertisements and electronic media ads, the overwhelming majority use the telephone.

According to the National Fraud Information Center,[9] the top 10 frauds during the year 2000 were:

Prizes and Sweepstakes	18%
Magazine Sales	14%
Credit Card Scams	13%
Work at Home	10%
Advance Fee Loans	9%
Telephone Slamming	7%
Credit Card Loss Protection	4%
Buyers Clubs	3%
Telephone Cramming	2%
Travel/Vacations	2%

As is evident, all of these fraudulent callers pretend to be selling a product or service. They close the sale, ask for a credit card number to pay for it, but never

deliver. Some are very insidious, such as the credit card loss protection plans. They ask for the victim's credit card numbers and expiration dates, sign them up, then disappear. The same approach serves to gather valid credit card numbers for fraudulent purchases by scam rings.

Various others con the victims into thinking that they're receiving something of value, but the items are non-existent. The work-at-home scams are typical. The seller offers the victim an opportunity to earn a lot of money by working at home a few hours a day. The "catch" is that the victim must pay a registration fee, or pay for materials, or pay an enrollment fee. Once the victim pays, he waits, and waits, and waits.

The vacation scam works by telling the victim he's won a very attractive vacation, but must pay the taxes or some other fee. Often, the vacation is mythical, and once the victim pays, he never collects. In other cases the "vacation" has so many exclusions as to be worthless. The package does not include transportation, food, or entertainment, but is merely a voucher for a hotel in a distant location. This is merely a variation on the prizes and sweepstakes fraud, in which the fraudster tells the victim he's won a prize in a contest he never entered.

The Computer Software Scam

A telephone caller informs you that you've won a computer software package, and asks you questions about your computer on the pretext that he must en-

sure compatibility with your system. Once he's got you hooked, he asks when someone will be home so that his company may deliver it. The whole point of the exercise is to obtain your schedule, and find out when nobody will be home, so he can schedule a burglary at your home.

Credit and Credit Repair Frauds

These are designed to victimize the marginal people in our society, the minimal earners who are not too bright and have run up large credit card balances or have acquired poor credit ratings because they didn't manage their money. One type is the loan-for-a-fee scam, in which the victim is offered an unsecured loan but must first send in a "processing fee." Although the scammer promises that the loan is guaranteed, no loan ever materializes. The more considerate ones refer the victims to a "turndown room," from which a staffer explains that the loan application has been turned down.[10]

Credit "repair" services take advantage of those with poor credit ratings by promising to fix their bad ratings. They claim to be able to remove derogatory records, such as bankruptcies, foreclosures, and the like from their victims' credit records. Naturally, there is a fee for this service, and after the victims pay, they find that their credit histories are the same as before.[11]

Credit Card Offers

Some scammers operating on the telephone offer people credit cards with unrealistically high limits or impossibly low interest rates. Others offer credit cards to people with credit ratings so poor that other providers have refused to approve credit cards for them. These offers are attractive, but the catch is that the consumer must send an immediate payment for a "processing fee" or other purpose. Once the sucker sends his money, either by mail or paying with a credit card over the phone, he'll wait forever for his new card to arrive.

This is an outright scam, compared to the relatively legitimate offers by established credit card providers. These send out offers of initially low interest rates. However, after several months, the interest rate jumps. One canny lawyer decided to take advantage of such an offer. He accepted a credit card that offered him a $50,000 line of credit for six months at one percent interest. With this, he bought a six-month certificate of deposit that paid him six percent. At the end of six months, he'd made a profit, using the credit card company's money!

Telephone Service Frauds

Telephone companies are into making money like other businesses, and at times they cut corners to earn more. One common scheme used by long-distance carriers is "slamming," switching you from your pre-

sent carrier and signing you up for their service without your consent or even knowledge. This can happen when a telemarketer for a long-distance service, eager to earn his commission, falsifies your assent and signs you up even though you've refused. Another trick, used by the company itself, is to mail you a check. If you cash it, they've "Gotcha" because the fine print on the back says that by endorsing the check you're signing up for their service.

Another tactic is "cramming," charging you for services you didn't order. Telephone companies slip these onto your phone bill, hoping that you won't notice.

One tactic that is perfectly legal is the pre-paid phone card that is more expensive to use than the regular telephone rates. This tactic depends on customers' not reading the fine print.

Another legal tactic is the hotel telephone that charges higher than average rates for calls. Most hotels offer free local calls, but bill the guests for long-distance calls. The hotel obtains its long-distance telephone service for guest telephones from a company that charges a very high fee and pays the hotel a commission on every call made by guests. Again, the success of this trick depends on the customer's not asking what the rates are before placing his call.

At times, the telephone company literally has a captive clientele. Many jails and prisons provide telephones in cellblocks for the use of inmates. These are wired to a telephone company that allows only collect calls. An inmate calling out has to get the other party to accept the collect call, and the charge for this is ex-

orbitant. In turn, the telephone company pays a commission to the jail administration for each call.

Cellular Phone Frauds

During the 1990s fraud artists counterfeited the chips in cellular phones, capturing genuine identification numbers by using receivers to pick up cellular phone transmissions. They'd set up shop near a busy intersection, knowing that many drivers would have their cellular phones turned on as they drove by. They would then program these genuine numbers into chips that they would install in their own phones, a technique called "cloning," and they would rent them to people who wanted to make long-distance or international calls. Technical improvements in cellular phones defeated some of these efforts, but now there's a new wrinkle.

This ties in with credit card fraud. Today, it's more difficult than ever to forge a credit card from scratch, because their manufacture and their security features are designed to make forgery extraordinarily difficult. Credit card fraud artists have resorted to securing genuine credit cards by using other peoples' identities. In the same manner, cellular phone scammers now use stolen identities to obtain cellular phones to use in their schemes. This points up the importance of safeguarding one's identity and identity documents. Practicing security in this way can prevent more than one type of fraud. Let's look at credit card fraud next.

Notes

1. http://www.fraud.org/telemarketing/teleinfo.htm
2. Pearson, Mike, *Waging War From Canada*, Port Townsend, Washington, Loompanics Unlimited, 2001, pp. 41-71.
3. *Ibid.*, p. 74.
4. *Ibid.*, pp. 92-93.
5. *Ibid.*, pp. 23-39.
6. *Ibid.*, p. 167.
7. *Ibid.*, p. 75.
8. Fleck, Caroline, "Buyer Beware: Scams Proliferating," *AARP Bulletin*, October 2001, p. 3.
9. http://fraud.org/telemarketing/statsfinal.htm
10. http://www.usdoj.gov/criminal/fraud/telemarketing/schemes.htm
11. *Ibid.*

Chapter Four
Credit Card Fraud

It used to be that physical possession of a credit card was necessary for a fraud. A pickpocket or burglar would steal someone's wallet for the cash it contained, and sell the credit cards to a professional credit card fraud specialist, who in turn would use them to purchase goods and services. This specialist knew that he was in a race against time, until the victim realized that his card was missing, so he would rush to get as much out of the stolen card as possible before the victim had it cancelled.[1]

Today, the great majority of fraudulent credit card transactions do not involve or even require physical possession of the card because they're conducted over the telephone or the Internet. All the fraudster needs is the card number and expiration date, and this is available from a discarded credit card receipt or even a carbon. As we noted before, the Internet and the telephone have made remote-control transactions quick and easy, and eased the way for fraudsters.

Some credit card fraud artists use a card reader and a computer to make electronic duplicates of stolen credit cards. They first use the card reader to pick up the information on the card's magnetic stripe, then use it to record the information on the magnetic stripes of other cards.[2] This method allows them to re-use the same cards as they steal new credit cards.

We've seen that there's a need for speed when working with a stolen credit card. Service stations with "pay at the pump" are perfect outlets, and some fraud artists drive in vehicles with extra-large gas tanks so that they can "buy" a large amount of fuel, often for later resale.[3]

Another common credit-card-related scam is the credit card protection plan, which purportedly protects the subscriber against potential losses if he loses his credit card or it's stolen. This type of protection plan is superfluous because federal law limits the cardholder's liability to $50 in such cases.[4]

The Feds Get Ripped Off Too

Federal employees who receive government credit cards are tempted to charge personal purchases to them. Some, such as an employee of the Los Angeles U.S. Attorney's Office who charged half a million dollars in personal purchases, give in to this temptation. Some Department of Education employees used their cards to pay for Internet pornographic materials.[5]

Government executives, as well as some lower-level employees, receive credit cards for their convenience,

to pay for legitimate on-the-job expenses. The purpose was to speed purchases by cutting red tape. One outstanding example is the gasoline credit card for those driving government vehicles. Some of these use the cards to fill up their personal vehicles.

The problem has developed into a multi-million dollar abuse because of the great number of credit cards issued, and the difficulty in monitoring all of them for irregularities. The Pentagon has issued 1.8 million credit cards to its employees, some having several credit cards at the same time. The Department of the Interior has 82,835 cards to serve only 68,000 employees. In theory, all credit card purchases leave paper trails. In practice, it's necessary for auditors to go over them carefully to detect improper purchases. Modern technology has made this impossible in some cases.

Before "pay at the pump" became common, anyone buying gasoline would receive a credit card slip, with the vehicle license plate recorded on it if the gas station employee was conscientious. Today, the driver just swipes his credit card through the pump's card reader, and the receipt only records the number of gallons, the price, and the credit card number. It's impossible for an auditor to know if a particular fuel purchase was for a government vehicle or a privately owned one.

Of course, stupidity can trip up a government employee who uses his government-issued credit card fraudulently. One who fills up his motor home's tank will create a record of a gas purchase much larger than the tank capacity of the government sedan he

uses. Another who runs up bills at an Internet porn site can expect an auditor to question it.

While stand-alone credit card scams are flourishing, many fraud artists are into a more complicated scheme, identity theft.

Notes

1. Daniels, Dave, Certified Communications Security Professional, *Credit Card and Identity Fraud Scams*, p. 1.
2. *Ibid.*
3. *Ibid.*
4. Fleck, Caroline, "Buyer Beware: Scams Proliferating," *AARP Bulletin*, October, 2001, p. 3.
5. Pace, David, Associated Press, "Feds Slow to Find Card Abuse," *Albuquerque Journal*, August 15, 2001, p. A5.

Chapter Five
Identity Theft

Identity theft is a type of crime in which someone wrongfully obtains another's personal data in order to use it for fraud. Briefly, the identity scammer gets hold of your data and applies for credit cards in your name or otherwise uses the information to charge purchases to you.

The growth of identity theft is a result of the increasing security of identity documents, credit cards, checks, and other sensitive documents, to prevent forgery. Years ago, a skilled forger could duplicate almost any type of document using an assortment of papers, cards, inks, and stamps. A photo ID such as a passport would require a camera as well. Today, it's much more difficult to forge a document from scratch. A driver's license, for example, may contain several of the following security features:

- The driver's photograph is in color, and is laminated into a plastic card.

- The card has a "security overlay" with a hologram of the name of the state or a design that is hard to reproduce.
- The card has a bar code on the back.
- The card has a variable graphic film laminate that displays the name of the state when tilted against the light.
- The state seal, flag, or other symbol is in ultraviolet ink over part of the photograph.
- The driver's license number's first two digits correspond to the driver's year of birth.
- A magnetic stripe is on the back of the card. This may contain a digitized photo of the driver, the driver's digitized signature, and a reproduction of the information on the front of the license.
- A ghost image of the driver's photograph is under the descriptive information.

All these features combine to produce a driver's license that is a nightmare to forge or alter. Other sensitive documents also contain security features. Checks are printed on special paper and have ink patterns that fade if exposed to bleaches used to remove ink. Given all this, it's much easier to obtain genuine documents using a pretext than to attempt to forge or alter them. The result is identity theft.

Identity theft is an ever-growing problem, fed both by organized crime and by small operators. Because identity theft is so easy, it's become a criminal cottage industry as well as a tool for complex scams involving large criminal organizations. It's hard to say exactly how much money is lost each year as a result of iden-

tity theft, but estimates run into the hundreds of millions of dollars, depending on the source. The FBI claims that identity thieves steal about $800 million per year. Actually, these "estimates" are mainly guesswork, but all are high, showing that identity theft is a serious and growing problem.

Traditionally, identity theft was a technique used by criminals and spies to conceal their true identities. They would "take over" the identity of another person and use his name in their daily movements to avoid detection. They would obtain driver's licenses and passports in that name, and could lead parallel existences without their victim's becoming aware that he had a paperwork twin. The Soviet spy Konon Molody used the identity of a Canadian, Gordon Lonsdale, to establish himself in England and lead a spy ring for several years. His assumed identity carried him through until British security officers uncovered the spy ring. Identity theft was also used by Soviet "illegals" in the United States, who took over the identities of American citizens. We also saw this technique used in fiction. The novel and movie, *Day of the Jackal*, showed how a political contract killer took over the identity of a British citizen, who had died in childhood, to obtain a passport. After French police had discovered this identity, he used a passport stolen from a Danish schoolteacher to continue his effort to kill President de Gaulle. Today, however, identity theft is much more sophisticated, more common, and is almost entirely profit-driven.

At present, there are at least 500,000 cases of identity theft a year, and there's every reason to believe

this number will grow. There are many avenues to stealing another's identity, and self-protection requires a basic understanding of the methods.

Stealing your personal data requires stealing your personal documents in most cases. They can steal your wallet or purse. They can steal your mail, either by raiding your mailbox or filing a change of address form with the post office to divert your mail. They can also get hold of your personal documents, such as bank statements, by "Dumpster diving," or stealing them out of your garbage. Any personal information you keep in your home can become the target of burglars. Now let's look at a few cases to see how some of these identity thieves operate in the real world.

A former University of Akron (Ohio) professor received a 16-month jail sentence for defrauding friends and neighbors of $115,000 via credit card fraud. After acquiring the Social Security cards and driver's licenses of friends, he obtained credit cards in their names and made expensive purchases on these accounts. He also used a credit card that had mistakenly been sent to him.[1]

This was an example of a single operator exploiting targets of opportunity. Other instances appear to be group efforts, as in a recent rash of Puget Sound area mail and identity thefts that authorities say are linked to "loose-knit groups of manufacturers, sellers, and users" of methamphetamine. Their method of operation involves stealing checks and other financial documents from mailboxes and using them to make purchases in their victims' names. The least sophisti-

cated way is to bleach the ink on a check, then make it out to another payee and for a different amount. A more elaborate technique used by the thieves is to obtain driver's licenses, birth certificates, and other IDs in the victims' names.[2]

One woman who operated an identity theft ring began by setting up mailboxes along rural routes. She also took mail from other people's mailboxes. Some of the items she stole were bank statements, credit card statements, checks, and other financial documents that provided their victims' account numbers. Members of the ring then sent the banks and credit card providers change of addresses, so that they could divert the statements and keep their victims unaware of the thefts. They secured checks and credit cards for their own use, using their victims' names, and proceeded to run up bills right to the limit.[3]

Identity theft is popular with people newly arrived in this country, as well. Three men from the Ivory Coast and Burkina Faso, in Western Africa, were arrested following a traffic stop in New Mexico after the officer found fake passports and immigration documents in their vehicle. They allegedly told agents that they were going to use the fraudulent documents to obtain real Social Security cards, but it was unclear what the end result would be. However, this sort of document scam points to identity theft.[4]

Identity theft victimizes both the person whose identity is stolen and the companies from whom the thieves make purchases of goods and services. Expedia, an online travel office owned by Microsoft, has suffered millions of dollars' losses at the hands of peo-

ple who purchased online travel using stolen credit card numbers. State Farm Insurance found that an identity theft ring used a stolen identity to purchase automobile insurance, then staged accidents and filed fraudulent claims. This is an example of identity theft overlapping into insurance fraud.

Identity theft feeds other kinds of criminal activities. A few such are computer fraud, loan fraud, election fraud, food stamp fraud, money laundering, securities fraud, student loan fraud, cellular phone fraud, and worker's compensation fraud. Auto loan fraud is particularly profitable, as the scammer can purchase a vehicle using the victim's name, drive it away, and resell it for an immediate profit.

Identity Theft and Terrorism

At times, profit is not the motive. Some of the terrorists who conducted the airliner attacks on the Pentagon and the World Trade Center on September 11, 2001, used the identities of innocent citizens of Saudi Arabia and other Middle Eastern nations. One uninvolved person stated that he had had his passport stolen some months before the attack. As the investigation will take months or years to complete, it's unclear what other methods of identity theft were used by the perpetrators.

However, other enterprising scammers have taken up the effort in the wake of the attacks. Families of some of the missing persons in the World Trade Center attacks had placed their relatives' names on post-

ers, hoping that someone would be able to provide information about their kin. Nassau County Executive Thomas Gulotta warned that scammers had telephoned families of victims and asked for personal information about the victims, information that would be useful for identity theft. He went on to advise families of missing persons not to give out information over the phone.[5]

Identity Brokers

It doesn't take a rocket scientist to use a stolen identity to purchase goods and services. The procedure is exactly the same as ordering with a genuine credit card. The front-line scammer, however, often lacks the knowledge and skill to purloin another's identity. This lack of skill points up the need for a specialist, the identity broker.

There are fraud rings that don't directly practice fraud using stolen identities, but sell them to other fraudsters. This is a new cottage industry and is very lucrative and safe because the identity broker is not in the front line of fraud and therefore less likely to be detected. An identity broker with a large network of outlets can enable thousands of fraudulent accounts, with a resulting loss of millions of dollars.

It typically takes little capital and resources to set up an identity broker business. A small group of skilled con men can operate with little overhead, working by word of mouth to obtain customers. These con artists establish a network of contacts, through

trusted references, thereby organizing a steady client base for their products, stolen identities.

One reason the identity theft business is so profitable is the previously mentioned low overhead. Identity brokers don't set up corporate headquarters in the same way a legitimate business does. They don't have the advertising expenses of legitimate companies. They operate out of rented premises, such as apartments, where they also live, further cutting the overhead. Some even operate from motel rooms and automobiles, which affords them mobility. A moving target is hard to hit, and this is an effective countermeasure against law enforcement.

Mobility is important to a fraud artist of whatever stripe. Mobility enables the scammer to stay a step or two ahead of the law. Here's how:

Police often attack crime rings by apprehending one member and persuading him to reveal his contacts and associates in return for a reduced sentence. This can work if police can locate the contact. However, if the identity broker relocates frequently, he can be very elusive. A policy of "Don't call us. We'll call you" can break the crucial first link in the chain, and make it very difficult for police to work back along the line to locate him.

One weakness of identity brokers is their propensity to maximize profits by recycling the identities they sell. They'll sell a stolen identity to more than one end-user. This often alerts credit card companies to fraud, as the same person is very unlikely to be paying for purchases from two different locations. An ob-

vious example is renting two motel rooms in widely separated places the same evening. In the same manner, an end-user is tempted to maximize his gain by ordering two or more credit cards or cellular phones, for use by accomplices.

Credit card and cellular phone providers use this to obtain early warning of fraudulent accounts. A sudden increase in purchases or use is a tip-off that there is more than one user, or that a fraud artist is trying to maké maximum use of the account before the victim or provider discovers the fraud.

In cellular phone fraud, a tip-off is the "test call." The scammer is likely to make a call on that phone just to verify that the account is operating. If the fraud artist intends to use the cellular phone for international calls, he will likely call the weather service or information in the other country to avoid linking the phone to a number that might lead back to him. In other words, he's not likely to call a friend or associate in another country just for verification. There may also be a delay of a day or more between the test call and beginning regular use.

Cellular phone providers can (and probably do) program their computers to highlight a pattern of calls to the same number, in or out of the country, by many different accounts. If the calls also include multiple calls by the same account using two or more phones, this is another red flag.

Congress Reacts

In 1998, the U.S. Congress passed the "Identity Theft and Assumption Deterrence Act," 18 U.S. Code Section 1028. This is the normal and expected reaction of legislators, who see passing another law as the solution to every problem. Legislators are limited to appointing committees to investigate problems and passing laws to eliminate them. The noted American psychologist, Abraham Maslow, characterized such a situation this way: "When your only tool is a hammer, every problem begins to look like a nail."

Passing a law to ban one type of criminal activity is one thing. Enforcing the law is another. As we've seen, the Identity Theft Act has had no discernible effect in stopping identity theft.

Identity theft is not the only problem. Other scams are on the scene. Some are new, while others are variants of old frauds. Let's look at these next.

Notes

1. Caniglia, John, "Ex-Professor Gets Prison for Fraud," *Cleveland Plain Dealer*, June 20, 2001.
2. Skolnik, Sam, "Meth Use Linked to Jump in ID, Mail Thefts," *Seattle Post-Intelligencer*, July 23, 2001.
3. Pilcher, Debbie, "Postal Inspector Cancels Woman's Crime," *The Cleveland Advocate*, July 11, 2001, www.zwire.com/site/news.cfm

4. Contreras, Guillermo, "Three Men Arrested in Social Security Scam," *Albuquerque Journal*, August 17, 2001, p. B2.
5. "Con Artists Seeking Missing Persons Data," *Albuquerque Journal*, September 29, 2001, p. A5.

Chapter Six
Charities, Down and Dirty

The terrorist attack of September 11, 2001, saw a surge of charities appealing for support to benefit the victims and their survivors. Both legitimate charities and fraud artists joined the effort, avidly collecting money and other donations as the American people gave very generously. It soon became clear, though, that some of the charitable appeals were outright frauds, and that none of the intended recipients would ever see any of the money that had been scammed from the American people. Not long after, it also became clear that some of the legitimate charities were following their own agendas, manipulating Americans into giving in the belief that it would all be used for the stated purpose. There arose a serious crisis of confidence in the traditional, legitimate charities.

The dividing line between legitimate charities and fraudulent ones is becoming ever more blurred. The relentless drive to raise money by any means has changed the character of many traditional charities,

and we have seen several charity scandals during recent years. This is why we have to study the history and the methods of charities, and how their fund-raising efforts are often much like those of fraud artists. We'll also see that contrary to what they may claim, some divert money from the intended use.

The 20th century saw the rise of many charities collecting money for various worthy causes. Today, there exist well over a million "non-profits," serving a variety of causes. Many are strident in their appeals for funds, using high-pressure tactics that would be condemned if businesses used them. They place advertisements showing photographs of starving children to tug at the heartstrings of potential contributors. This takes advantage of the sympathy many Americans have for children, as con artists know that an appeal to help children is irresistible for many. Others enlist armies of volunteers to canvass their neighbors for donations. What many contributors don't know is that many charities are basically fund-raising organizations devoted to assuring a comfortable lifestyle for their top executives and headquarters staffs, and that much of the money collected never reaches the intended beneficiaries.

Fund-raising is a specialized trade, and there are companies that offer training in how to raise money for various purposes. Most of their clients are "non-profit" organizations that enjoy special tax exemptions because their activities are theoretically not for profit. These fund-raising consultants train non-profit organizations in various techniques to persuade peo-

ple to donate money. They outline various avenues of approach, such as newspaper advertisements, direct mail, telephone canvassing, and the use of volunteer fund-raisers.

Non-profit organizations attain their special status because they are not directly involved in operating for profits that they pass on to owners and stockholders. This differentiates them from for-profit entities such as General Motors and Lockheed-Martin, which are companies that sell their products for profit and pay dividends to stockholders.

Non-profit organizations are organized the same way as for-profit companies. They have chief executive officers and staffs, and as in their for-profit counterparts, their executives are well paid. Their executives also enjoy expense accounts and opulent offices. The main differences are that their executives are not quite as well paid, and do not enjoy stock option plans.

The largest for-profit companies have Chief Executive Officers (CEOs) who pull in salaries of tens or hundreds of millions of dollars a year. By contrast, the largest non-profits have top salaries of only a few hundred thousand dollars annually. Perquisites of office differ as well. Large companies have executive jets equipped with the latest navigational aids and other expensive features, and these small luxury aircraft have very comfortable seating, meeting rooms, bars, galleys, and other creature comforts. Most charities do not have such conspicuous benefits for their CEOs.

Funds collected by legitimate charities do not all go to the intended purpose. It costs money to rent office space, pay for postage, advertisements, etc., and a portion goes to administrative overhead and collection expenses. These are legitimate expenses, depending on how much money they devote to overhead in proportion to what they collect.

The American Institute of Philanthropy is a watchdog organization that rates charities according to standards it has developed. These standards center around how the charities handle the money they collect. It maintains a Web site to inform those who want to know how much of the money they contribute actually goes to help the needy.[1]

How much of the money collected should actually go to charitable programs? The AIP considers that 60 percent or greater is reasonable. The rest goes for fund-raising and administrative expenses. This benchmark is important because many charities spend a lot more money on expenses, and actually are not very effective in funneling money to those who need it. In some cases, as little as 15 percent goes to the cause, and the rest is swallowed up by fund-raising costs, salaries, overhead, etc. The recent example of the September 11th fund-raising for charitable purposes is a good example. Let's take a quick look at some of the problems that have appeared.

Daniel Borochoff, President of the AIP, testified before Congress on November 8, 2001, that some charities spend 20 percent or less of their collections on the advertised need. He also pointed out that some of the

charitable efforts resulting from the terrorist attack of September 11, 2001, are duplicating the efforts of various levels of government. Some fundraisers stated that they were raising money to help the families of police officers and firefighters who lost their lives that day. However, widows already receive tax-free lifetime pensions amounting to the officers' full salary, as well as $151,000 from the U.S. Department of Justice and $25,000 from the New York City Mayor's Office. Officers' unions also pay out death benefits. Many people who gave to these charities did not know about these benefits.[2]

Borochoff also discussed the American Red Cross, which was the subject of controversy because of its fund-raising and what it did with the money raised. He pointed out that the Red Cross has an "A" rating for "spending 90 percent of its total expenses on program services and having a cost of only 15 percent to raise $100." He went on to say: "The concern in this disaster is that it is spending money on areas other than what was most heavily advertised and perceived to be the need by the public that being the direct victims, their family and the relief workers. Even if the Red Cross keeps to its $320 million budget, it is likely that less than half the $550 million raised will be used for this purpose."

He also stated that the United Way has distributed only one tenth of the $340 million it had collected, although it had earlier claimed that "100 percent of all contributions to the September 11th fund are being used to help the victims, families, and communities affected by the terrorist strike." Borochoff pointed out

that some of the money collected by United Way was given as grants to other non-profits "that may spend some of this money on overhead costs."

The AIP Web site posted a special alert regarding fund-raising in relation to the September 11th terrorist strike. It warned readers to "Restrict or designate your contributions for this specific crisis. If you do not, there is a risk that the charity will use your donation for a different purpose." It also warned to be cautious regarding donations to police and firefighter groups, and to check with local police or firefighters first to determine their legitimacy.[3]

The AIP rates an organization's efficiency, the amount of money it spends in direct fund-raising costs. The AIP standard is that no more than 35 percent of the money raised should go to fund-raising costs. In other words, no more than $35 should go to raise $100. However, some charities use other ways of calculating this ratio. They list their fund-raising expenses against total income, which can also include patient revenue, investment income, and sales proceeds. For example, the American Red Cross sells blood to hospitals. Other charities invest some of the money they collect. Yet other non-profit groups sell promotional materials. DARE, for example, sells banners, bumper stickers, tee-shirts, and other items, and raises money this way. So do other non-profit organizations.

Also important are the funds available in reserve. We've seen that many charities do not spend all of their money on charitable purposes, but put some

aside in investments, possibly to carry them through lean fund-raising periods. The AIP standard is that a charitable organization should have no more than three years' reserve.

All of these factors go into the AIP's ratings of charities. The ratings range from A+ to F, with F being the lowest. Some of the charities rated A+ are:

Elizabeth Glaser Pediatric AIDS Foundation
American Indian Graduate Center
Cancer Research Institute
National Childhood Cancer Foundation
Child Welfare League of America
Conservation Fund
Hispanic Scholarship Fund
National Alliance to End Homelessness
International Rescue Committee
National Mental Health Association
Fund For Peace

The AIP warns that a rating system does not tell the whole story. Accounting audits can be erroneous or misleading, which is why it advises that before you give, you should check out a charity thoroughly. Reputable charities provide information on their operations, especially where your money goes.

The Better Business Bureau also has a set of standards for charities. These standards include providing an annual report on request, as well as complete annual financial statements. Financial statements must include a description of income sources, expenses broken down into categories such as solicitations, salaries, employee benefits, etc.[4]

Very important in the BBB's set of standards are charitable fund-raising and the proportion used for the intended purpose. A "reasonable" percentage of funds collected should go for the intended purpose, and the BBB defines "reasonable" as 50 percent of total income to be spent on directly related programs and activities. It also states that fund-raising costs should not exceed 35 percent of the total. The BBB standards also state that solicitation materials should be truthful and accurate, and that the organization be prepared to substantiate their accuracy. There should be a clear description of how the funds are to be used. There is also a clear prohibition against publicizing the identities of donors without prior written permission. In other words, this bans selling "sucker lists."

The governing structure should also be adequate, according to the BBB standard. There should be articles of incorporation and bylaws, established by the organization's governing board. The governing board, or board of directors, should meet at least three times a year to establish policies and oversee their implementation, and a majority of board members should attend. This is to avoid the practice of listing the names of prominent people as board members solely for the prestige. Also important is the independence of board members, and boards with more than 20 percent of the board members receiving any sort of compensation do not meet the standard.

It's important to know something about a charity that asks you for money. Never give money to any

charity that keeps its cards close to the vest. Secretiveness is ample cause for suspicion.

Ask if the charity is registered with a government agency. Any non-church charity that has an annual income of more than $25,000 must register with the Internal Revenue Service. So must any charity to claim tax-deductible status. Likewise, 36 states require charities to register with the appropriate branch of the state government.

Always ask where your dollars go. Ask the charity what percentage of your contributions goes for overhead and administration. Find out what percentage goes for fund-raising costs. Look carefully at any expenses listed as "public education," as this is an accounting ploy used to disguise large fund-raising expenses. Judge this on a case-by-case basis, because charities are inconsistent in self-reporting. In other words, charities don't balance their books the same way.

Obtain a copy of its financial report. Don't take "no" for an answer. Any refusal to provide a copy is automatically suspect, whatever the excuse may be. With the report in your hand, read it carefully, including the fine print designed to make perusal tedious. After all, it's your money. What do you look for?

- Check how much it costs the charity to raise funds. Although the standard mentioned by the AIP and the BBB is 35 percent, you may feel that this is too high. How much of its money actually goes for its intended mission? Does the money go directly to

the people it's claiming to help, or does it get channeled through several other organizations?

- The financial report should also list its operating expenses. How much does the charity's CEO receive in salary? Is this reasonable to you? Search for the expense account. How much does the CEO receive for travel and other expenses? Look for loans to directors, trustees, and the charity's officers, as this is a red flag that funds are not going where they should. Note especially the term of that loan, if listed, and ask about them if they're not. Look for interest-free loans, or loans at rates below prevailing ones.
- Do any members of the charity's governing board have any business relationships with the charity they oversee? This could be a conflict of interest, or an indicator that money is being diverted for private use. A red flag is a contract for products or services by a board member's company. This could mean that office supplies, for example, are being sold at inflated prices. It could also be a "retainer" paid to a board member who is an attorney. Always determine exactly what services are received for that "retainer." Another red flag is a "consulting fee" paid to any board member or former officer. "Consulting" is a vague term used to cover a tenuous, vague, or non-existent service.

Learn to resist pressure. If you don't know the charity, ask for more information, and get it in writing before sending any money. Pressure tactics are the warning sign of fakers. Remember that you're in the

driver's seat because they want your money. Insist on having your questions answered fully before opening your checkbook.

Always make contributions by check or money order, so that you have a record of your contribution. One obvious reason is to be able to deduct your contributions on your income tax return. Another is that cash can easily disappear into the pocket of the fund-raiser. Yet another reason is that giving out your credit card number to a telephone solicitor is dangerous. You truly do not know who the person on the other end of the line is. This is especially true if your Caller ID shows "Out of Area," "Private Call," or "Blocked Call." Anyone can telephone you and pretend to be from a reputable charity, just to get your credit card number.

Beware of charities that send you gifts. Some will mail you personalized address stickers, greeting cards, and other cheap gifts to build up a feeling of obligation. You may feel that you have to send them something to cover at least the cost of the "gift." Always remember that the cost of such "gifts" can increase the costs of fund-raising. Also remember that it is illegal for a person or organization to demand payment for unordered merchandise.

What Happens After People Contribute

Estimates of the amount of money collected by legitimate charities after the WTC attack range from $700 million to over $1 billion. A lot of money was col-

lected during a very short time. One obvious point is that the families of the victims are seeing very little of it.

The total dead from the attacks is about 3,000. A quick calculation shows that $1 billion should have resulted in $333,000 per family of the dead. In reality, the families have received very little money from the legitimate charities. At best, the non-profits are very quick at collecting money, but very slow at handing it out to the needy.

Besides money appeals are the many appeals for blood by legitimate organizations. Ostensibly, blood donations were to aid survivors of these attacks, but although it became clear after a couple of days that there were few survivors, the appeals continued. The reason is that blood banks sell human blood for a fat profit, something they don't tell people who come in to donate blood.

In the wake of the World Trade Center attack, the American Red Cross collected a tremendous amount of blood, much more than would be needed to take care of the injured. The Red Cross sold some of the surplus to hospitals. The eventual aftermath was that the Red Cross discarded thousands of pints of the surplus blood collected, because whole blood has a limited shelf life and the Red Cross did not have enough freezer space to store it. Red Cross officials did not answer questions about how much blood they had collected.[5]

The American Red Cross, a legitimate charity, collected a lot of money and blood donations in the af-

termath of the World Trade Center attack. So did the United Way. Daniel Borochoff, President of the American Institute of Philanthropy, pointed out that the United Way had handed out only ten percent of the $87 million United Way had collected. This brought up the question of the interest collected on the $87 million, and what happened to the interest.[6]

The American Red Cross admitted to having collected $564 million for its "Liberty Fund," set up as a result of the World Trade Center attack. As of November 7, 2001, the Liberty Fund had paid out $121 million to victims of the attacks and their families. However, $6 million of the money went for administrative costs, and the Red Cross earmarked another $50 million to set up a "strategic blood reserve." Fourteen point seven million went to public education and mental health counseling. The Red Cross stated that $264 million are for a reserve fund against general terrorism and anthrax threats.[7]

It's clear where some of the money goes. Bernadine Healy, former President of the American Red Cross, earned $450,000 per year. This is more than twice the salary of the President of the United States.[8]

The firestorm of criticism was so intense that the Red Cross reversed its position on November 14th and stated that all of the money collected would go to victims' families. The new CEO, Harold Decker, announced the move after New York Attorney General Eliot Spitzer had said he was prepared to sue the Red Cross.[9]

Some Sidelights

As we've seen, some of these organizations hand down money to others. Each layer in this "trickle-down" process absorbs a percentage of the funds for administrative expenses. By the time the money trickles down to those who really need it, there's not much left.

A number of celebrities helped raise money for various charities in the wake of the September 11 attacks. Fund-raisers bring the entertainers involved a lot of publicity. It may be uncharitable to conclude that the entertainers are more interested in their images than in helping people, but Bill O'Reilly brought up this thought in his "Talking Points" of November 1, 2001. He had contacted the public relations agents (flacks) for many of the entertainers who had participated in concerts for charities and asked them what responsibility they had in seeing that the charities handled the money honestly. Most flacks answered that their clients were too busy to make a statement. Others provided various excuses for not commenting, such as one not being able to make a statement because his wife is pregnant.

Businesses

Some private businesses used the World Trade Center angle to promote their products. Makers of flags and other patriotic symbols saw a sudden surge in orders. However, some enterprising businesses went a

step further. One art dealer, the Island Illusions Art Gallery, stated in its Internet ad that it would donate ten percent of all art sales to either the American Red Cross or the National Disaster and Search Dog Organization. This is not illegal, but you might want to give your contribution directly to the charity instead of channeling it though a for-profit business.[10]

Web Sites

Many legitimate charities have Web sites, but these are not always adequate. Few legitimate charity Web sites include financial reports. Instead, they concentrate on appeals, sales of merchandise, and information on the cause they support. This is why it's important to be very careful before donating money over the Internet.

Competition Between Charities

One of the little-known aspects of established charities is the frantic scrambling for funds. There is only so much money to go around, and the many charities compete for it. The volume of 9-11 donations resulted in less money being available for other charities not directly involved with disaster relief. World Neighbors, a charity that works with the rural poor, stated that their donations had dropped by 77 percent. The Los Angeles Society for the Prevention of Cruelty to Animals also experienced a loss of mail-in

donations, and as a result was planning to lay off some employees and close facilities.[11]

This points up the importance of checking out any charity or non-profit organization before you give. Don't give your money impulsively, in a rush of emotion, because the scammers are counting on this. In addition to the established charities, there is a rash of outright frauds, and we'll study these in the next chapter.

Notes

1. www.charitywatch.org
2. www.charitywatch.org/congress.html
3. www.charitywatch.org/alerts.html
4. Give.org, BBB Wise Giving Alliance, www.give.org/standards/cbbbstds.asp
5. "Red Cross Knew Blood Unusable," *Albuquerque Journal*, November 11, 2001, p. A4.
6. *The O'Reilly Factor*, Fox News, October 9, 2001.
7. McCaffrey, Shannon, Associated Press, "Red Cross Defends Use of Funds," *Albuquerque Journal*, November 7, 2001, p. A11.
8. Farhi, Paul, *Washington Post*, "Red Cross President Criticized in Wake of Attacks," *Albuquerque Journal*, October 26, 2001, p. D1.
9. McCaffrey, Shannon, Associated Press, "Red Cross Reverses Decision," *Albuquerque Journal*, November 15, 2001, p. A9.
10. http://www.islandillusions.com/911.html

11. Kiesling, Donna, "9-11 Donations Exact Price on Other Charities," *The Star*, October 7, 2001. www.star-newspapers.com/star/spnews/all/07af8.htm

Chapter Seven
Fake Charities

This scam is as old as the hills, but it's still with us, made more common and more effective by telemarketing. Asking for funds in the name of a spurious charity takes advantage of our good nature, and it's very profitable. Often, the charity scammer will use a name that sounds like that of a real charity devoted to helping children, victims of various illnesses, etc. Beware of any telephone caller claiming to represent a familiar charity. It's hard to tell real charities from fakes these days because there are so many genuine charities that keeping track of them is almost impossible.

An especially vicious aftermath of the terrorist attacks on the World Trade Center and the Pentagon is the rash of bogus charities piggy-backing on real relief funds. The attack brought out the best in some people, and the worst in others. While TV stations, banks, and other legitimate organizations have established funds to aid the victims of these disasters, fraud art-

ists have been telephoning people to solicit contributions for their fake funds.[1]

This type of fraud scheme isn't new. Telescammers react quickly to developing events. There had been bogus charities soliciting money after the Oklahoma City bombing and other disasters. The U.S. Department of Justice has established a special Web site to inform the public about fraud schemes stemming from the terrorist attacks of September 11. Fraud artists are soliciting donations for victims of the attacks via e-mail as well as the telephone, asking people to send their credit card numbers and other personal information to Internet Web sites. Some have claimed to be representing the American National Red Cross and other charitable organizations. The Web site is: http://www/usdoj.gov/criminal/fraud/WTCpentSpecRpt.htm.

The Department of Justice goes on to stress that legitimate organizations do not ask for Social Security numbers, passwords, PIN numbers, etc.

Other World Trade Center related frauds involved slightly different tactics. One caller claimed to represent the Reader's Digest Sweepstakes and told one victim that although he had won, disruption of the U.S. Postal Service made delivery of her prize impossible. He asked for $2,500 to speed delivery, according to the National Consumers League.[2]

Another potential victim received an e-mail asking for donations to finance a group of computer experts engaged in locating Osama bin Laden. He was asked to send money to a bank account in Estonia.

Another person found a message on his answering machine asking for help in raising $1 million to help victims of the disaster. When he tried to call the number back, he reached an answering machine for a telemarketing company he didn't recognize.

Other callers selling magazine subscriptions claimed to be associated with Publishers Clearing House. Some of these used a name that sounds familiar, such as "Publishers Clearing Service," or "Publishing Clearing House." They told their intended victims that part of the proceeds would go to help victims of the September 11 disaster.

Some con men preyed on family members of missing persons or those identified as casualties. These sold fake mementos from "Ground Zero." In response to this, New York Mayor Rudolph Giuliani said that each family would receive from the city, at no charge, soil from Ground Zero in a wooden urn.[3]

Insurance companies found themselves hit by bogus claims stemming from the disaster. The National Insurance Crime Bureau reported claims of accidents involving cars that weren't even in the area, and claims for cars supposedly lost in the rubble. Insurance companies are anticipating a flood of scammers trying to obtain money under false pretexts.[4]

The World Trade Center attack also resulted in a rash of investment scams. Telephone callers offered offshore "safe haven" investments for those who could be persuaded that American markets are going down hard. Of course, sending money to another country to be "invested" is very questionable, and can easily result in the loss of all the funds.

Other telephone scammers touted commodities, offbeat financial plans, and companies producing new anti-terrorist technologies. While there are legitimate companies involved in the development of anti-terrorist technologies, these are unlikely to solicit investors by cold calls.

The Securities and Exchange Commission took action against one allegedly illegitmate company during early November 2001. It suspended trading in 2DoTrade Inc.'s stock "because of questions about the accuracy of the company's claims, the status of its business operations and prospects, and the identity and backgrounds of people running the company." The Nevada company had stated in its latest SEC filing that it was in the retail and restaurant business. The company had stated in a press release that it was testing an anthrax disinfectant, but a telephone number listed to the company had been disconnected and a public relations spokesman declined to comment. The SEC added that investors should treat with skepticism the claims of companies stating that they are producing a product effective against terrorism.[5]

The American Association of Retired Persons issued a warning about terrorist-related scams. These include fraud artists claiming to represent police or military organizations seeking funds for the troops, fake war bonds, or flags for children. Others are phony insurance policies trading on fears of terrorist attacks. Another is the scammer telephoning to collect personal information "to replace records lost in the collapse of the World trade Center." Fraud artists also

had collected money while claiming to represent the American Red Cross and other charities.[6]

Scammers sometimes justify themselves by quoting the old saying, "You can't cheat an honest man." By this, they try to claim that the only reason they can perpetrate their frauds is that deep down, their victims are as venal and dishonest as they. Charity scams prove that this is false. Fraud artists appeal to victims' altruism when they use the fake charity trick.

Notes

1. NCIX Website Update Advisory #18-2001.
2. http://www.nationalconsumersleague.org/disasterscampr.htm
3. Stashenko, Joel, Associated Press, "Survivors Will Receive Urns of WTC Soil," *Albuquerque Journal*, October 3, 2001, p. A5.
4. Beamish, Rita, Associated Press, "Lies Rise From N.Y. Wreckage," *Albuquerque Journal*, October 16, 2001, p. C5.
5. Gordon, Marcy, Associated Press, "Terrorism Cures May Be Phony," *Albuquerque Journal*, November 7, 2001, p. B7.
6. Barry, Patricia, "Scams Swiftly Follow Terrorist Attacks," *AARP Bulletin*, November, 2001, pp. 24-25.

Chapter Eight
Airline Security Scams

Airline security began as a response to a rash of "skyjackings" during the 1960s, when some political skyjackers took over commercial aircraft and had their pilots fly them to Cuba and other places. The FAA and the airlines set up security checkpoints at the entrances to boarding gate concourses, and hired unarmed private security guard agencies on contract to staff the checkpoints. The checkpoints consisted of metal detectors and conveyor belts that passed all carry-on luggage through X-ray machines to detect weapons.

Private security puts profits ahead of performance, and the companies involved hired low-level people at minimum wage or slightly above minimum, to put on a show of security for the public. Skyjackings abated, but probably not as a result of the increased security but because skyjacking had simply been a criminal fad that soon went out of style.

During the following years, airline security became very perfunctory, actually a farce. Passengers complained that metal detectors slowed boarding by forcing them to stand in long lines, while they emptied their pockets of keys and coins that made the buzzers sound. Meanwhile, airline security failures became conspicuous. The loss of Pan American Flight 103 to a terrorist bomb showed that the security system was not only far from perfect, but very porous.

The Gulf War brought a re-appraisal of airline security, and critics were quick to compare lax American security to that conducted by El Al, the Israeli airline. This was a poor comparison, because El Al is a small airline, with about three dozen aircraft, while American carriers send thousands of flights aloft each day. One major American airline carries more passengers in one day than El Al carries in a year.

A few "reforms" came into play. At some airports, curbside check-in of luggage stopped. Security guards turned up the sensitivity of their metal detectors. Research began on explosive detectors to warn of bombs placed in luggage. All of this was cosmetic, and proved to be ineffective on September 11, 2001, when a group of terrorists hijacked several airliners and flew them into the Pentagon and the World Trade Center in suicide attacks that left about 3,000 people dead and two major New York landmarks piles of rubble.

Over the years, private security operators at airports had been found negligent by Federal Aviation Authority (FAA) inspectors and fined millions of dollars. This did not help the problem, because the pri-

vate security companies paid the fines and continued business as usual. After the terrorist attacks, security at airports was supposedly beefed up but violations continued. This time, they drew national attention because of the seriousness of the situation. Reporters for *The New York Daily News* tested security at several airports on the East Coast, including Boston's Logan Airport, where some of the September 11 skyjackers took off, and found that they were able to slip weapons by the security checkpoints. A man boarded an airliner in New Orleans carrying a pistol.

In theory, airport security staffs were supposed to check luggage for explosives using high-tech explosive detectors, but in practice this did not work well. "Fewer than 10 percent of checked bags at the nation's airports are inspected for bombs, and one overworked detection machine operator was found falling asleep on the job," according to the Transportation Department's Inspector General in testimony before Congress.[1]

Meanwhile, the illusion of security continued. Armed National Guard troops were posted to guard airports, and Congress wrangled over whether to keep airport security guards as employees of private contractors or make them federal employees. A program of background checks on people hired by private security companies showed that some were convicted felons.

Airline security is a sham. The security system is so porous that it's ineffective. With thousands of flights daily, it's almost as difficult to make the airlines secure as it is to make subways safe. If you board an air-

liner and arrive safely at your destination, it's because nobody tried to skyjack it.

Should you fly commercial airlines? The same factors that make it almost impossible to make airliners safe work to minimize the odds of your aircraft being skyjacked and destroyed. There are too many of them. It would take an army of terrorists to commandeer all of the airliners flying in one day. You have a better chance of being killed in a traffic accident than of being killed while flying.

Notes

1. Abrams, Jim, Associated Press, "Lapses Continuing In Baggage Security," *Albuquerque Journal*, November 15, 2001, p. A8.

Chapter Nine
Miscellaneous Frauds

Information Fraud

A group of scammers devised a new fraud based on current "politically correct" trends to defraud senior citizens into disclosing personal information that the scammers can use for identity theft. The group printed leaflets promising black seniors payment of $5,000 in "slave reparations" if they sent documentation of their status, including birth certificates, Social Security numbers, and other personal documents and data, to a post office box in Washington, DC. The post office box was in the name of the TREA Senior Citizens League. Other leaflets promised money to "notch babies," born between 1917 and 1926, falsely claiming they were eligible for payments of $5,000. The scam artists "piggybacked" on the name of a legitimate organization, The Retired Enlisted Association (TREA).[1]

A variation on this theme is when a fraud ring member works in a hotel or restaurant, and copies a

guest's name, credit card number, and expiration date. A member of the ring telephones the victim later, posing as a credit card company employee, and asks him to confirm the transaction, which of course the victim does. After having gained the victim's confidence this way, the fraud artist obtains further information, which the ring uses to steal the victim's identity.

Cross-Border Sweepstakes Fraud

Phony sweepstakes have been with us for a long time, but a new development is the crossing of a national boundary. The new sweepstakes fraud artists have refined their scheme to maximize their returns while minimizing their risks. Some Americans have received notices informing them that they have won prizes in sweepstakes they never entered. They are told that, to collect their prizes, they must send a check for between $20 and $30 to a Canadian address, always a mail drop.[2]

The notification letters go out from U.S. addresses, probably to avoid suspicion by U.S. postal officials who might be scrutinizing mass mailings originating from out of the country. It's also very easy to spread mass mailings around several local post offices to avoid creating an obvious pattern.

Using a Canadian mail drop means that it's harder to coordinate a multi-national investigation. Law enforcement across national boundaries is always very tenuous, and the investigations become very cumber-

some. This is true even between neighboring countries, such as the United States and Canada, and few investigations result in prosecutions. This is why these schemes include many variants, such as prize-promotion schemes, lottery frauds, etc. In many cases follow-up and prosecution of fraud artists across national borders is very slow and involved, despite extradition treaties, and the scammers get away scot-free.[3]

Lottery Scams

Although federal laws prohibit importing lotteries or running them across state lines, lottery scammers ignore these. They contact potential victims by telephone, mail, or via the Internet. The scammers sell lottery tickets, at first for five or ten dollars, meanwhile compiling a list of receptive people. Later, telemarketers passing themselves off as lottery experts contact the most promising victims and ask them to invest substantial amounts. In reality, little or no money is invested because the telemarketers keep it for themselves. These fraud artists operate by effrontery, and in the rare instances when victims have learned that their number had won, they did not pay out any money, telling the victims that they had reinvested their winnings in more lottery tickets.[4]

At times, the lotteries seem like "Ponzi" schemes, in which collections from future victims are used to pay off early "winners." It's not too hard, and it's a good investment, to convince the most gullible and affluent

victims with small prizes that they're on winning streaks and to encourage them to lay out even more money.

The "Gimme" Gift

Passing off junk as valuable items is common in fraud schemes. The fraud artist contacts potential victims by telephone and tells them that they have won a prize. He does not specify exactly the prize won, but reads from a list of prizes, most of which have substantial value. Prizes include an automobile, a check for thousands of dollars, and other desirable items. Sandwiched between them is a junk watch, or pair of watches, or cheap gold rings. This is the "gimme" gift. Once he has the victim hooked, the scammer tells him that he must buy certain goods or send in a processing fee to collect his prize.

Effrontery is the key to the scam, and if the victim asks which gift he has won, the fraud artist fobs him off with double-talk that informing him would be "collusion" and illegal. In practice, victims only receive the cheap items, never the valuable ones. This is why the scammers insist on payment in advance, before the victim sees the "gimme" gift and realizes its true value.[5]

Home Repair Scams

These are not new, but they've had a revival during this new century. The basic scam works like this:

The fraud artist goes door to door and tries to persuade homeowners that their roofs or driveways need repair. The con man then takes the money and leaves without performing the work, or he uses sub-standard materials and performs a faulty repair. There are variations on this theme, and one is to tell the homeowner that the "contractor" is working on another house down the street and has materials left over. The con man offers to do the job at a discount to avoid having to haul the surplus material back to his shop. Another con is to offer to do the work at a very attractive price, then charge more when the job is finished.[6]

Some of these con artists are very hard to catch because they hit and run. They'll work an area on one day, and the next day they're in the next state. This is another instance of mobility enabling the con artists to remain a step ahead of law enforcement.

The Missing Pets Scam

Owners of missing pets who put up posters offering rewards to those who return their pets may become victims of a hard-hearted scam. The fraud artist telephones and says he has the pet, and asks that the reward money be wired to him via Western Union. Of course, he does not have the pet, and once he gets the money, the pet owner never hears from him again.

This scam has two characteristics that tip you off the caller is a phony. First, for one pretext or another, the caller cannot meet you in person to hand over your pet for the money. The second tip-off is that he

wants you to send him the money via Western Union, because he can pick up the money anywhere in the country, preventing you from tracing him. Western Union does not require identification, unless the sender specifically requests it. When one victim did this, the scammer called back to say he had lost his wallet and asked that the victim change the order to "no identification required."[7]

The Gerber Food Name Scam

A group of fraud artists placed advertisements stating that the Gerber Baby Food Company has lost a class action lawsuit, and that the parents of children under a certain age should send copies of their children's birth certificates and Social Security numbers to a certain address. This is a trick to obtain basic information for identity theft.[8]

The "809" Scam

The "809" Scam, dating from the last decade, still thrives because of a lack of uniform laws across national boundaries. It's particularly serious in telecommunications, where each nation has its own procedures, and fraud artists are quick to take advantage of conditions that figuratively allow them to get away with murder. Area Code 809 is listed for the Caribbean, and you don't have to dial a country code to reach it. The caller is unaware that he's dialing outside the United States. Scam artists operating in the

British Virgin Islands set up "pay per call" numbers there to receive calls from the United States. Local laws allow them to charge almost any amount they wish, and a typical rate is $25 per minute. The way they victimize you is to leave a message on your answering machine that a family member has been arrested or is ill. When you call the number given, you hear a recorded message designed to keep you on the line as long as possible. When you receive your phone bill, you'll see it contains an astronomical charge. You have no recourse, because you actually did place the call. Your local telephone company won't want to get into the middle of this, stating that they're merely passing on billing from another company.

There are variants on the "809" Scam that have sprung up during the last couple of years. Instead of a message on your answering machine, you may find a number beginning with "809" on your pager. You may also receive an e-mail directing you to phone an 809-number because you've won a prize, or a company is offering you lucrative employment.

Pyramid Marketing Scams

These are schemes that recruit people to become "sales managers" or "distributors," promising rich rewards for little work. The victim has to invest his own money to buy stock and recruit other people to sell it, receiving a commission on the amount of product sold. The product may be genuine or a fraud itself, such as a miracle cure for baldness.

Typically, the scammer will hold a high-pressure meeting or seminar attended by many prospective victims. The fraudster will razzle-dazzle his victims by showing charts purporting to list the amount of money it's possible to earn by recruiting other people to do the actual selling. The fraud artist promises that the product is easy to sell, and that the victim will find it easy to recruit and supervise a sales staff with little effort. Sprinkled through the audience are shills to provide testimony of how easy the plan is, and how much money they have earned. Other shills go through the motions of enrolling themselves in the plan, because the scammer knows that most people are cautious and reluctant to be the first to sign up for the plan. The method of operation is to build up emotional momentum with these shills, and make it appear that people are enthusiastically signing up for the program.

Nigerian and Similar Frauds

During the last several years we've seen the "Nigerian Scam" proliferate, with many people stripped of their liquid assets. The classic Nigerian fraud involves a letter or e-mail to a prospective victim, promising a quick and generous return if he provides the scammer with his bank account numbers. The scammer says he needs American bank accounts to allow him to transfer by wire several million dollars he scammed from the Nigerian Government. Once the scammer has the victim's account number, he "vacuum-cleans" the ac-

counts by means of bank drafts, and the money is out of the country, gone forever.

There are many variations on this scam. Some fraud artists will send you letters, e-mails, or faxes purporting to come from an official of a foreign government. To support their claims, some scammers will include letters of recommendation from American companies. They may also ask you to provide, along with your account numbers, blank letterheads from your company, your telephone, fax, and e-mail numbers, and other information. The blank letterheads are to allow the scammers to forge recommendations from your company. As with many frauds, the perpetrators will stress the "confidentiality" of the transaction, to deter you from going to the authorities or consulting your attorney.

The appeal can take different forms. One variant is to offer you a piece of a real estate venture. Another is offering you the opportunity to purchase bulk quantities of crude oil at very attractive prices. Other techniques are to tell you that the writer is the beneficiary of a will, or recipient of an award. Once you show interest, they sink in the hook and ask for front money so that you may collect your share of the proceeds. Your money is to pay for taxes, attorney fees, customs fees, bribes, etc. In each instance, the scammer assures you that this is a temporary problem, and that paying the fee will allow the deal to proceed. However, there's always another problem arising that requires you to front more money until you get tired of laying out money for no visible return.

At times, the scam can involve a threat to your freedom or even your life. You may receive an appeal to come to Nigeria to finish the deal. The scammer will tell you that you can enter the country without a visa, as he'll take care of bribing a Nigerian immigration official. As entering Nigeria without a visa is a serious offense, this can be used against you, as leverage to ensure your compliance with whatever demands the fraud artists make. If you refuse, your life may even be in danger, as one American was murdered in Lagos, Nigeria, a victim of this scam. Other foreign nationals who have traveled to Nigeria following up on these fraudulent offers have not been heard from since.

A variant on this theme victimized the former Finance Director of the City of Clovis, New Mexico, who was approached by people claiming to be members of the Ugandan Rebel Army. They promised him a quick return for investing $4 million of city funds with them. The former city official was convicted of falsifying public documents in the fall of 2000, received a suspended sentence, moved to Arizona, and committed suicide with carbon monoxide in August, 2001.[9]

The U.S. Secret Service has established a special office within its Financial Crimes Division to cope with Nigerian scams. "Operation 4-1-9" involves liaison with Nigerian and other police agencies to try to stop the scams and to prosecute the scammers. The operation gets its name from the section of the Nigerian Penal Code dealing with frauds. The Secret Service also has several of its officers in Lagos, Nigeria, to col-

laborate with Nigerian officials in prosecuting scams. However, this is only a drop in the bucket for a very simple reason. "Nigerian" scams may have originated in Nigeria, but they've spread to other countries. Scammers using variations on the Nigerian themes are now working their schemes from several other locales, and catching up to them is difficult because they change locations often.

There's an additional reason why Nigerian-type frauds have proliferated. Typically, law enforcement authorities are concerned with crimes in their own jurisdictions, not others, and even less concerned with crimes against people of other countries. The police of Nigeria will be less than enthusiastic about investigating a fraud ring that targets Americans. The parent body, the national government, of an underdeveloped country can easily turn a blind eye to a criminal ring that brings sorely needed money into the local economy. Until there is a world police force, there will be little hope of combating fraud across national boundaries.

Work at Home

Work-at-home schemes are not new, but some scammers are using the telephone and the Internet to attract victims. These scammers promise big bucks for little effort in a variety of businesses. They also assure their victims that success is almost guaranteed. The plans usually involve setting up a network of vending machines, computer games, or recruiting

other salespeople. If recruiting other salespersons is part of the plan, it's a pyramid selling scheme, as discussed above. All require that the victim purchase equipment or stock from the scammer.[10]

Stock and Bond Frauds

A classic type of fraud still being perpetrated because prosecution is so difficult is stock analysts' benefiting financially from touting stocks. This is a variation of the "pump and dump" technique used by stock fraudsters for years. The main differences are that the perpetrators are employees of "respectable" firms, and the stocks and bonds they tout are "reputable," not junk.

A stock analyst decides to invest in a particular issue he thinks is worthwhile. After sinking his money into it he advises his clients that it's a good buy, and when they buy shares the purchases drive the price up. Once the analyst feels it has gone as far as it's going to go, he sells his shares, thereby profiting from the transaction.

What's wrong with this picture? The analyst is using other people's money to drive up the price of the shares. However, as many have discovered, proving intent is very, very difficult. A federal judge recently dismissed a lawsuit brought by investors against an analyst working for Morgan Stanley, showing that winning a case is not the same thing as the feeling that you've been victimized.[11]

There has been a rash of lawsuits recently by investors who had allegedly lost millions of dollars by following the advice of stock analysts who did not reveal that they had conflicts of interest. One reason is that the stock market has taken a downturn. Investments appeared rosy when the market was bullish, when almost anyone with money to invest saw a profit, and predicting a stock's rise was almost a no-brainer. Today, though, stocks that are basically feeble or overvalued are crashing, and taking investors with them.

Some fraud artists are pitching worthless stocks by phone, using a variation of the Initial Public Offering theme. An Initial Public Offering, or IPO, is the first time a company's stock is put on the market. The company establishes a selling price, and from there the stock may take off and appreciate in value on the market, or it may decline in value or even crash. IPOs are inherently risky because the stocks have no track record.

The pre-IPO fraud is slightly different. The fraud artist may be a telemarketer, or operate by e-mail or on the Internet. He offers the victim a "pre-IPO" deal, an opportunity to buy shares before they go on the market. The victims are not aware that there's no guarantee of an initial public offering, and that the stock they're contemplating buying may never go on the market. Although the scammer offers the victims both low risk and high return, the offer is bogus.[12]

Unclaimed Estates

At times, people we normally think of as being above suspicion turn into scammers. A former minister in Florida pleaded guilty to defrauding the Florida Department of Banking and Finance of over $1 million. The first step in the fraud was to buy a state database listing unclaimed estate property. This was openly available over the Internet and on a CD-ROM. He then used faked identities to claim some of these estates from the state. According to U.S. Attorney Thomas F. Kirwin, the scammer then used the money to buy himself a 6,625 square foot house, motor vehicles, other property, and computers. He also established several bank accounts with the proceeds of the scam.[13]

Religion-Based Scams

These tend to be aimed at older people, and use their religious beliefs to take money from them. Many people think that any offer associated with a religion must be good, and scammers take advantage of this naïve belief. Scam operators tout various investment schemes, such as precious metal and diamond mines in Africa, claiming that the investors will receive a generous return and that part of the profits will go for a worthy cause, such as a non-existent church. Another religion-based fraud is perpetrated by fly-by-night "clergymen" who claim to be raising money to build their churches.[14]

Recovery Room Frauds

Adding insult to injury is a sophisticated two-tiered fraud practiced by some scammers. After fleecing their victims with one type of scam, they pass their names to another group, a member of which contacts the victim and claims to be associated with a law enforcement agency. The "agency" may be local, state, or federal, and may be a police agency or a prosecutor's office.

The pitch is that the "agent" will attempt to recover some of the funds lost by the victim. Because the "agent" is working in collusion with the original scammers, he is well informed regarding the type of scheme used and the amount of money lost. This helps convince a credulous victim that the "agent" really is associated with law enforcement. The "agent" then sinks in his hook, informing the victim that there is an up-front fee involved because there is a court filing fee and their funds must be released by the court.

Using the "recovery room" scam has two benefits for the bold scammer. It allows him to steal yet more money from his victims, and it can delay the reporting of the scam to the real authorities if the victim believes that something is already being done.[15]

Fake Experts in the Media

It's become a feature of American life that the news media aren't here to bring us an unbiased view of national and world events, as we'd learned in our civics

classes. Today, anyone who doesn't have his head in the sand acknowledges that the real purpose of newspapers, radio news shows, and TV news shows is to capture audiences for advertisers. The neologism "info-tainment" summarizes it well.

One aspect of info-tainment is to describe and explain an increasingly complex and bewildering world for audiences. This taxes the skills of the "talking heads" on the regular news staff because of their limited knowledge. In certain cases, they bring in outside help. We have seen how the electronic media do this regularly, with guest speakers, and the TV news are the worst offenders.

It's very understandable when a TV station puts a medical doctor on screen to describe and explain a new technique of endoscopic surgery, or a new antidepressant drug. In the same manner, an attorney might appear to describe the implications of a new law or court decision. However, experts aren't always that well qualified. A recent example shows what can happen, and why it's important for you to be skeptical about the views of some of TV's "experts."

The new war against terrorism brought an unprecedented crop of specialists and "experts" to comment on terrorism, national security, and the military actions in Afghanistan. Typically, these were retired military officers who answered questions from the talking heads. A few were college professors or employees of "think tanks" dealing with security topics. Some were asked for their views on terrorism and anthrax, while others were asked to explain the United State's mili-

tary goals or bombing campaign. In some cases, the talking heads even asked them to predict what would happen next.

Retired military officers aren't privy to current war plans. Even if they were, they would not disclose them, as they'd face prosecution for revealing military secrets. Indeed, Defense Secretary Donald Rumsfeld berated some people in the government (mainly members of Congress) for talking out of turn and disclosing classified information.

When the topic turned to terrorism, the experts showed themselves as very uninformed, and they merely repeated stale clichés regarding terrorism. The reason is very clear. Retired military officers are experts on their former services, not terrorism. Practically all of them had never even seen a terrorist. This is why it's important to be skeptical when faced by one of TV's "experts."

Fraud Marches On

You and many other people are besieged daily by fraud artists. Under this continuous assault, is there anything you can do to protect yourself? The answer is "YES!"

While there is no technique or combination of techniques that offers 100 percent protection, you can make it very hard for a fraudster to take advantage of you. That is the subject of the rest of this book. There are steps you can take, individually and collectively, to enhance your resistance to fraud, and there are

steps your government can take to combat fraud on the international level.

Notes

1. Sprengelmeyer, M. E., "Senior Citizens Duped Out of Personal Data," *Rocky Mountain News*, July 10, 2001.
2. http://www.bbb.org/alerts/sweepstakes.asp
3. http://www.usdoj.gov/criminal/fraud/telemarketing/schemes.htm
4. *Ibid.*
5. *Ibid.*
6. Fleck, Caroline, "Buyer Beware: Scams Proliferating," *AARP Bulletin*, October, 2001, p. 3.
7. Morrison, Keith, "Double Tragedy for Pet Owners," *NBC News*, July 20, 2001.
8. Verizon Phone Fraud Alliance, "Gerber Food Scam: True Name Fraud."
9. "Ex-Clovis Director Commits Suicide," *Albuquerque Journal*, August 17, 2001, p. B3.
10. http://www.usdoj.gov/criminal/fraud/telemarketing/schemes.htm
11. Gordon, Marcy, Associated Press, "Deception Hard Thing to Prove," *Albuquerque Journal*, Sunday, September 2, 2001, p. C1.
12. Fleck, Caroline, "Buyer Beware: Scams Proliferating," *AARP Bulletin*, October, 2001, p. 3.
13. Associated Press, "Ex-Minister Admits to Fraud Counts," *Albuquerque Journal*, September 28, 2001, p. B2.

14. Fleck, Caroline, "Buyer Beware: Scams Proliferating," *AARP Bulletin*, October, 2001, p. 3.
15. http://www.usdoj.gov/criminal/fraud/telemarketing/schemes.htm

Chapter Ten
Protecting Yourself

From what we've seen, fraud artists are getting away with huge amounts of money, without facing a correspondingly high risk of apprehension or prosecution. Law enforcement is largely ineffective when it comes to fraud, because fraud artists are at least as smart as the cops, and know how to take advantage of weaknesses in the system.

Most police departments are unprepared to combat fraud. They can barely cope with street crime while an inept criminal justice system sabotages what the cops accomplish. No doubt, you've heard the cliché: "Send for a cop, then send for a pizza. See which comes first." Unfortunately, this isn't a myth. It's true in many parts of the country.

It's worse when it comes to fraud. Often, the cops don't come at all. If you receive a suspicious telephone call from a fraud artist, don't waste your time calling the police to ask them to trace the call. You'll just ex-

perience a run-around while the fraudster moves on to other victims.

If the cops can't protect you, then who can? It comes down to self-reliance. You are the first line of defense against fraud, just as you're your own first line of defense against street crime.

A cliché is that some of the sharpest minds in the world are working on the problem of separating you from your money. The smartest of these are concentrating on doing it by stealth and deceit, not by force. This is why you must remain vigilant in your daily life. You must also know a few basic survival tactics.

Security

Let's first look at some very basic precautions that many people neglect. One is to keep your wallet in a safe place, such as an inside pocket that you can button. This is especially true if you're female. Don't carry your wallet full of cash and credit cards, and perhaps your checkbook, in your purse. Purses are too easy to snatch. A thug can snatch your purse and be off running before you can react.

Also, never leave your wallet, purse, checkbook, or cellular phone in your car. You might think you're safe by leaving them under the seat, but someone may be watching and break a window to steal them later. Also, if your car gets stolen, your valuables get stolen with it.

Another basic safety tactic is never to write your PIN number on your credit card or ATM card. Don't

even write them on a slip of paper in your wallet. If you do, you make it very easy for anyone who steals or finds the cards if you lose them.

Memorize the numbers. This isn't hard to do, if you do it correctly. Don't use your house number, birth date or any number linked to you as a PIN number. Instead, use a number you know, but that has no connection to you. The last four digits of a friend's telephone number are good to use. So is your friend's house number. Another might be your supervisor's office number or telephone extension. No scammer can possibly know all the people you know, and know all of their house or telephone numbers. Even if he did, finding the right one would be a mind-boggling task.

At home, keep your blank check pads in a safe place. If you have a safe, use it. If not, choose a hiding place that would take a thorough search to find. There's no perfect defense against burglary, but you don't have to make it easy for a burglar.

Be especially careful if you live with roommates. They may not be what they seem, especially if you don't bother to check them out first. One man found that a former roommate had purloined a check from the bottom of his blank check pad, and used it to clean out his account.

Be Suspicious

It's smart to be suspicious of someone making you an offer or urging you to buy or invest in something. Always "consider the source." As noted above, anony-

mous messages on Internet message boards or chat rooms are always suspect because you don't know the source. These messages are usually posted by shills. In the same manner, be careful when someone solicits contributions for charities with which you're not familiar, or with names that sound like real ones. Check it out before sending any money. However, being suspicious does not mean going overboard and becoming a paranoid, distrusting everybody you meet. A healthy degree of suspicion is important for defense against fraud, and it should begin with asking, "What does he get out of this?"

When dealing with a salesman, the answer is obvious. The salesman is seeking to earn a commission. However, it's important to note that some people earning their livings this way don't call themselves "salesmen." Your stockbroker, for example, is actually a salesman, not a "financial advisor," because he earns a commission from every transaction. This is a strong incentive for him to persuade you to buy and sell securities.

Believe it or not, your health care provider is also a salesman. He stands to earn a fee for every treatment. This is a compelling reason to seek a second opinion if a doctor or a dentist proposes an expensive course of treatment.

One woman suffering from spasms of her right eyelid found this out the easy way. The doctor she consulted suggested she have expensive plastic surgery to correct the condition. This was a serious prospect, because of the risks associated with any surgery, and

she hesitated to accept the doctor's suggestion. In a few weeks, the condition cleared up by itself. She still doesn't know what had caused the condition, but her reluctance to accept this expensive "treatment" saved her a lot of money, as well as sparing her the surgical risk.

Regarding health care, be very careful about giving blanket permission to harvest your body organs. Scan very carefully any health care organization contract you sign, and be very careful regarding what you sign before going in for surgery. Likewise, do not check off the "organ donor" box on your driver's license application. While most doctors are ethical, you may have the misfortune to encounter one tempted to make some easy bucks by declaring you dead and harvesting your organs.

Read the Fine Print

Both legitimate businesses and scammers use fine print to fool people. A grocery ad will have a "SALE" price in large numbers, but the fine print below the price imposes a condition such as "Limit 4," "Thursdays only," or "Only to customers who buy $25 or more." The danger to you is that this tactic is perfectly legal, and if you get tricked, you have no recourse.

Be especially wary of offers that come in the mail. Credit card offers usually list a very attractive rate, but when you read the fine print you find that this is only for an initial period of a few months and that a higher rate then applies. You might be surprised to

find that the rate is higher than that on your present credit card.

If you receive an offer to enter a contest, read everything on the form before you sign it. You may discover that the "winner" has to pay a "service charge" or "processing fee." Be especially careful if you receive a check made out to you. It might be from your credit card provider, thanking you for being a valued customer, but scan it carefully. Always scan the back carefully for fine print saying that you're signing up for a service, magazine subscription, etc. One such check for $2.50 received by the author had printed in fine type on the front: "Cashing this check activates a risk-free 3-month membership in the Buyer's Advantage program with additional money-back privileges." There was no information on the check regarding how much membership would cost after the free offer expired. However, the accompanying letter stated that the annual fee would be $69.99 and would be automatically extended after the first year and billed to the credit card account. Very fine print at the bottom of the cover letter stated that motorized vehicles, food and beverages, jewelry, weapons, computer software, and many other items were excluded from the plan.

The above offer is not illegal, not technically a fraud, but it is a trap for anyone who doesn't read the fine print. Nobody gives away free money, and there's always a catch.

Another offer came from Fleet Instant Advantage Credit Card Services in the form of a check for $2,635.00. The accompanying letter reassured the

reader that the check was real, and urged the reader to deposit it immediately. Endorsing the check would activate a Visa Platinum credit card account. However, it was important to read the entire letter and the fine print on the back carefully to understand the terms.

The check wasn't a gift, but a loan, and the company expected repayment at an interest rate of 14.99 percent a year. The fine print on the back stated that there would be no grace period before interest charges would apply. In other words, there'd be a finance charge even if the client were to repay the entire loan upon receiving his first bill. If he did not, the minimum payment on this loan was $62.67 per month, over a term of 60 months. Simple arithmetic showed that anyone who endorsed and deposited this check would pay a total of $3,760.20 for the $2,645.00 loan if he took the entire 60 months to pay it back.

What's wrong with this picture? There's nothing illegal about it, as the letter with the check clearly states the terms, that the check is not a gift but merely a loan. The problem comes if someone steals the mail. The check is real, and it's negotiable. Although the check is marked "FOR DEPOSIT ONLY" a scam artist can open a bank account, deposit the check, and then work the scam one of two ways. He can receive a Visa Platinum card, if he has Fleet, send it to another address, enabling him to milk his victim's credit for many thousands of dollars. Alternately, the scammer could choose to take the money and run, withdrawing the balance a few days after

depositing the check. The victim would still be stuck with the loan.

The National Consumers League issued a warning about unexpected charges attached to buyers club memberships. Many of these are pitched by telemarketers, and these dishonest salespersons fail to tell victims that there is a charge after the introductory period. Other victims find themselves paying for memberships to clubs they'd never agreed to join. Yet another way victims get suckered in is by buying items advertised on television. Fine print on the screen tells them that the purchase automatically enrolls them in a club. Other victims said they'd received "welcome packets" from clubs even though they'd never applied for membership. When they tried to telephone to cancel these "memberships," they found that getting through was extraordinarily difficult.[1]

Another instance turned up in New Mexico, when Qwest, the area's telephone company, began a telemarketing effort to sell its wireless telephone service. Customers began complaining that the offer was misleading. Ken Graves, of the New Mexico Attorney General's Office, stated that "negative option contracts" are a growing problem.

A negative option contract isn't new. Actually, this is the way many book and music clubs operate. You have to notify the company that you don't want it, or they ship an item to you. Each sale period you receive a notice that if you do not return the card (using your

own stamp) within a certain time, you'll receive that month's book or tape.

In the case of the Qwest offer, the sales pitch was for a 30-day free trial. What the telephone salesperson didn't state, and the printed information provided in fine print, was that it was up to the customer to tell the company to cancel, or the customer would be committed to a year's service at $29.95 a month.[2]

Complicating the problem for the customer was that trying to contact Qwest via telephone meant a lot of waiting. One customer complained that she spent 90 minutes, mostly on "hold." Another difficulty was that the customer had to return the wireless phone within the specified period, but the phone arrived in a box with no return address.[3]

Coping With Telemarketers

Unless you're very isolated, you've gotten calls at inconvenient times from telephone salespeople. They tend to phone around dinnertime, because they know you're most likely to be at home then. Chances are they're using a computer programmed for sequential dialing, and dialing several numbers at once to save the telemarketer's time. If you receive "hang-up" calls, especially around dinner, it's almost surely a telemarketer, not a personal enemy trying to give you a hard time.

One counter to telemarketing calls is to tell each caller to place you on his "Do Not Call" list. Federal law provides penalties for telemarketers who continue

to call after being told this. In theory, you can file a civil suit against such a telemarketer. In practice, it's very hard to do so. You have to document your complaint, and unless you log every call you receive, noting the date, time, and caller, you won't get far.

Documenting calls is very difficult. Practically all telemarketers use PBX switchboards or other electronic trickery to prevent their numbers from registering on your Caller ID. A telemarketer can use a different name every week. This makes gathering evidence that will stand up in court very difficult. The telemarketing company simply denies it made the calls, and you can't prove that their personnel did.

Another approach is to contact the Direct Marketing Association and request to be removed from lists its members use. The number to call is:

New York: (212) 768-7277
Washington: (202) 955-5030

This again is only a partial solution. Telemarketers come and go, and when new ones spring up, they will call you. Another point is that fraud artists don't belong to this association, and call whom they please.

At the most basic level, protecting yourself from telemarketers is very simple: Never talk to them. There are several reasons for this. One is that it's a total waste of time. You have better things to do than explaining to a telephone salesperson why you don't want to buy. In any event, you don't owe a junk caller any explanation. Another is that if ever you buy anything from a telemarketer, your name and number will go on a premium "sucker" list and you'll be bom-

barded with even more calls. Be sure of one thing: They don't go away if you buy. You cannot appease them.

It's hard to exaggerate this point. Telemarketers, both legitimate ones and outright fraud artists, make money any way they can. One way is to sell lists of people who have bought from them, on the well-established premise that if a person's bought once, he'll buy again. Of course, they don't call these "sucker lists," but "lead lists," and the people on these are called "mooches," salesmen's slang for easy prey. In fact, there are list brokers who buy and sell lead lists to telemarketers and fraud artists. This shows that, in many ways, both honest and dishonest telemarketers operate in a similar manner.

Countering junk callers requires defense in depth, using several defensive layers. First is a Caller ID. Make it your practice never to pick up the phone if you don't know the caller. Don't let your curiosity make you pick up a "Blocked Call" or one that purports to come from "Out of Area."

There's a very good reason for not talking with junk callers, apart from the waste of your time. Some are totally unscrupulous. Other telephone junk callers are under such tremendous pressure to make their quotas that they will falsely write up your order. For example, some of the callers who try to get you to subscribe to their long-distance telephone services.

Telemarketers will also make misleading statements to entice a subscriber to make the change. The New Mexico Public Regulatory Commission heard testimony of such abuses from telephone subscribers. It

also heard testimony from a former employee of one of the long-distance companies that he and his fellow telemarketers "preyed on the elderly and made misleading statements to customers to meet high-pressure sales goals."[4]

It's become almost a cliché that scammers prey on the elderly. Is it because they're stupid? Probably not, as elderly people tend to be vulnerable for other reasons. First, they're home a lot more than people of working age, and therefore easier to reach by telephone. They also have savings and property, real assets that make attractive targets for fraud artists. Another reason is that they're more likely to listen patiently while the scammers make their pitches. They also may be less suspicious. Finally, many elderly people welcome telephone calls because they're lonely, and even sales calls help fill the empty hours. Whatever the reasons, people over age 62 make up the majority of victims.

Next you should get an answering machine so that you don't miss important calls, yet can turn away junk calls. A legitimate caller will leave a message. A caller who hangs up the moment your recorded message cuts in is surely a junk caller. An answering machine also removes the urgency involved in answering the telephone. If you're in the shower, washing dishes, or otherwise occupied, you don't have to drop everything to answer the damned phone, even if the caller is a friend. Finish your task and call the person back.

An answering machine can also provide the evidence to enable you to obtain justice. One rural New

Mexico couple took a call from one of these telemarketers, who was operating out of a call center in Kansas. When they refused to change their service, the telemarketer called again, allegedly leaving a nasty, profane, and threatening message on their answering machine. When the husband called the telemarketer's supervisor later that night, the supervisor denied that the incident had happened, until he heard the tape played. The couple hired a Santa Fe attorney and filed suit against the company.[5]

Finally, you can counterattack if you have the time. If, for example, you're on the toilet and have a phone in the bathroom, you have a few minutes to play with a telepest and waste his most priceless commodity, time. However, make sure you tape the call, to have a record of the conversation in case the telejunker later claims you bought whatever he's selling.

If a junk caller rings, there are several tactics you can employ to keep him tied up. However, don't use obsolete tactics. Asking the caller to hold because there's someone at your door is an old technique, and they're all aware of it. Likewise for telling him that you have someone on your other line. If you try it, you'll find that he's hung up when you return. To keep him on the line, you have to use a "hook," something to capture his interest.

Pretend to be interested in his offer. Listen, and ask questions. Pretend to be a little stupid, ask him for information he has already given you, and make him repeat himself a few times. Then tell him that you have to ask your spouse, and ask if he can hold for a minute. Put the phone down and continue reading the

newspaper, and after a couple of minutes pick up the phone and tell him that your spouse said "no."

If another family member is home, you can use the tag-team method on the caller. Tell him that his offer sounds very interesting, and that you'd like to have him run it by your spouse, or father, etc. The other family member gets on the line and puts the salesman through the same time-consuming routine, asking repetitious questions, before handing the phone back to you. Then you tell him that you want time to think about it. At this point, he may say that he'll phone you again the following day. Of course, the next day you simply don't answer any unidentified calls. Chances are that he'll try you several times before giving up, thereby wasting even more valuable time. Time is money to them, and by wasting their time you're hitting them right where they live.

Don't feel guilty about treating telephone pests this way. As we've seen, they have no scruples at all, and don't mind inconveniencing you with their calls and even lying when it suits their purpose. These scumbags deserve what you give them.

Following this simple program will make your life a little more peaceful. If you don't live alone, make sure other members of your family follow this program as well.

Learn to Say "No"

This is very basic, and is the heart of any fraud survival program. The fraud artist, as well as the legiti-

mate salesperson, will use any kind of pressure he can to get you to say "yes." However, remember that the fraud artist needs your cooperation, and this means that you're the one in control. Use this power to protect your interests.

Say "NO!" if anyone telephones you and asks you for your credit card numbers, their expiration dates, passwords, PIN numbers, bank account numbers, or any personal or financial information. There is no reason for a legitimate company or bank to ask you for this information by phone.

Also be wary of anyone telephoning you as part of a survey. You might be good-natured and want to be helpful, but remember that you're not obligated to help any stranger who telephones you. Also remember that you have only this person's word for it that the call relates to a legitimate survey, and that this might be a fraudster trying to obtain information from you for a scam. It also might be a cleverly convoluted sales call, with the "survey" used as a lead-in to a sales pitch once the caller has your attention.

If you really want to take part in the survey, ask for a call-back number. If it's a legitimate survey, the caller will have no objection to providing you with a number.

Another aspect of saying "No" is handling charity solicitations or other fund-raising appeals. Fund-raising has become a science in the United States today, and much fund-raising comes from computers that generate personalized letters. This is the sort of junk mail that crams your mailbox day after day, and

it takes time to sort the junk from the mail you really want to read.

Fund-raisers are adept at writing appealing letters, and they know that a certain percentage of people will respond to them. As with telephone solicitors, they won't go away if you try to appease them by sending a token amount. Most national organizations and charities send out fund-raising letters, first to their members, then to people on carefully selected mailing lists. Whether it's the National Rifle Association, the Republican Party, or some other organization, they operate pretty much the same way.

Some are more aggressive than others. Today, many fund-raising letters are disguised as "surveys," asking your opinion on a hot emotional issue such as abortion or gun control. When you get to the bottom of the survey form you find the "hook," a space asking you to list the amount of money you're sending to support the campaign.

If you send in a check, your name goes on a special list, and you'll find them pestering you for contributions more often. Send in another check, and you'll be hit by a barrage of fund-raising letters, and some of them might be from other organizations as well. If your name goes on a special "sucker list," distributed to other fund-raisers, you'll find your mailbox increasingly crammed with this sort of junk mail.

One retired university professor complained about the number of fund-raising letters that filled his mailbox. He sends contributions to about 80 charities a year, yet each day receives more appeals. The answer

was very simple. Some charities stated frankly, "The more we ask, the more people give."[6]

There is only one defense against a barrage of fund-raising letters. Never ever send in a contribution in response to any sort of appeal. Ignore fund-raising letters and you'll find that after a while the fund-raisers will begin to ignore you. Most of today's fund-raising letters are computer-generated, using a word processing feature called "mail-merge," that prints a personalized letter to everyone on a mailing list. Their computers are programmed to send out letters to everyone on the list, but to flag those who respond. After several letters in a row get ignored, the frequency of mailings drops sharply.

One active way to hurt these junk mailers is to open every envelope, looking for a business reply envelope. The "BRE" is pre-printed, and states that the recipient (the junk mailer) will pay the postage. Stuff this BRE with the promotional literature or other printed matter you have handy and mail it back to the junk mailer. The first-class rate for a BRE is more than the price of a first-class stamp. As with junk callers, you hit them where it hurts.

Don't Return Telephone Calls Blindly

If you find a message on your answering machine from someone you don't know, be careful about returning the call, as it might just be a come-on from a telemarketer. More seriously, it might be a costly scam if the number begins with the "809" area code.

As we've already seen, scammers in the British Virgin Islands try to entice you to call their numbers so that they can hit you with outrageous pay per minute charges, and they're very imaginative at dreaming up pretexts.

Likewise if you receive an e-mail telling you that you've won a prize, landed a job, etc., and asking you to telephone a number beginning with "809." If you find a number on your pager beginning with "809," ignore it, because it's sure to be a scam. Restrain your curiosity and save yourself a lot of money. In fact, it's a good idea to look up an unfamiliar area code before dialing it. Area codes are listed by location in the telephone directory.

Expect Surprises

Surprise is a basic tactic of the fraud artist. The scammer tries very hard to catch his victims unaware as he makes his play. The scammer will telephone you at home, or send you a letter. He may even approach you in person. In any event, he'll try to "hustle" you. This is why you must consider any offer or appeal very deliberately.

Don't Be Hustled

Make decisions deliberately, and don't let anybody rush or hustle you. The scammer doesn't want to give you time to think, to check up on him, or verify the validity of his offer. The fraud artist selling magnetic

pillows and blankets to relieve arthritis pain will tell you that magnetic therapy is supported by doctors, but he won't allow you time to check with your own doctor or to read about this therapy in medical books. He'll tell you that you must place your order right now to obtain the special price, and that the offer will expire at the end of the day.

Delaying the buying decision is one of the most effective methods of frustrating a scammer. If a telemarketer makes an offer to you, ask him for a number at which you can call him back. If he's legitimate, he'll have no reason to refuse.

Delay Tactics

Use any excuse to delay the decision:

"I'll have to ask my spouse. We always decide these things together." This works even if you're single because the caller doesn't know your marital status.

"I want to run this by my accountant" (or lawyer). This is another way to postpone the decision, and it puts pressure on any scammer because he knows an accountant or a lawyer is more likely to see the fraud than a lay person.

Yet another way is to take the time to look up the company or the offer on one of the Internet fraud sites listed in the chapter on "Resources." This imposes a delay in the proceedings, and it provides you the opportunity to obtain a solid reading on whether the offer or the company is legitimate.

"Can you send me literature on your offer?" Telling a caller or salesman you'd like to see it in writing is a powerful deterrent, especially if he's dishonest. It imposes a delay of several days while the material comes to you through the mail.

A scammer cannot stand a delay. Telling him firmly that you will not be rushed will often send him running, and this is a clear indication that the offer was not legitimate.

Use Your Common Sense

Always remember that an offer that appears too good to be true usually is. People are not in business to give way fortunes or to do you favors. If someone offers you a sure-fire "secret" way to get rich on the stock market, ask yourself why he's not using this secret to enrich himself, instead of wasting time trying to peddle it on the telephone.

Likewise if you're approached by a telemarketer telling you that you've "won" a trip to Europe, a cruise, or a car. How can you expect to "win" in a contest you've never entered? The offer becomes very suspicious if the fraud artist tells you that you have to send him money to pay a "processing fee," a tax, or another expense.

Also be very careful with charitable contributions. Scam artists appeal to people's better natures, and as we've seen, some are very agile in their quick response to events. The World Trade Center attack re-

sulted in a rash of appeals by legitimate and fake charities.

Never give money, or worse, your credit card number, in response to a telephone or e-mail appeal. It's best to give any contributions to the local branch of your favorite charity. If in doubt about any charity, call the Federal Trade Commission at (877) 382-4357.

Massachusetts law requires all charities and fundraisers to register with its Public Charities Division. This is a step towards making it harder for con artists to run charity scams in that state. Not all states have such requirements, which makes it very important to check out any charity several ways before contributing.

The Consumer Affairs and Business Regulation Web page of the Commonwealth of Massachusetts has a guide to precautions when considering charitable contributions. It advises obtaining lots of information from the charity, including where your money is going and how it will be used. It also advises asking for written materials about the charity, its purpose, and its finances. It's also important to obtain the exact name, address, and telephone number of the organization. This is probably the most important step in distinguishing between legitimate charities and outright frauds because the fly-by-nights are reluctant to give out any identifying information.

The Web site also cautions about similar-sounding names. Some fraud artists choose names that are very much like those of legitimate charities.

It's also important not to give cash contributions that could easily disappear into the pockets of the in-

dividual fund-raisers. Pay by check made out to the organization or by credit card, if you've verified that the charity is legitimate. This creates a paper trail authorities can trace if the charity later turns out to have been fraudulent. It also prevents dishonest employees of the charity from expropriating funds for their own use.[7]

Ask For a Call-Back Number

Tell a telephone caller that you'll have to call him back, and ask him to provide you with a number where you may reach him. Also ask for the name and address of his company. Any legitimate caller will be able to provide these. The fakes will not, and this is a good way to send them running.

Credit Card Protection

It used to be a truism to advise people to carry as little cash as possible to avoid losing it in case of robbery or losing one's wallet. Years ago, robbers and pickpockets were not very interested in credit cards because they did not see the potential, and cash was their preferred booty. Today it's very different, and one method of protecting your assets is to carry cash, not cards, in your wallet. A robber or pickpocket will get away only with the cash you have on you, and will not be able to loot your account for larger sums. If you absolutely must carry a credit card, keep it in another pocket, not in your wallet. Also, do not casually dis-

card sales receipts if you use a credit card for a purchase. Receipts often contain all the information a fraud artist needs to charge items to your account, or even steal your identity.

There's another advantage of carrying cash only. Businessmen know that a person with a credit card is likely to spend more than if using cash. The credit card doesn't seem like real money, and the credit card user knows that he won't have to pay until the end of the billing period anyway. On the other hand, someone paying cash knows that he's spending real money, and he's paying it at the moment of sale. Handling cash brings home the reality of spending money.

There's another tactic available to you to reduce the amount a scammer might steal using your credit card: Ask for a lower credit limit. If you charge only $500 or so each month, you don't need a $5,000 or $10,000 limit. A fringe benefit comes if you have a spouse who is a spendthrift and has a joint credit card account with you. A lower limit will prevent your spouse from delivering a nasty surprise with next month's bill.

Make sure you know the 800-number of your credit card company. It's printed on your card, but make a copy of it in case your card disappears. If you lose your card, call the number at once whatever hour of the day or night it may be. They're staffed 24/7 to take care of these problems, and can cancel your card immediately when you notify them of its theft or loss, or if you think someone else is running up bills on your account.[8]

Remember that today's credit card scammer doesn't need physical possession of your credit card to charge

purchases to you. This is why it's important never to recite your credit card number and expiration date to anyone who telephones you, whoever he claims to be. Remember that on the phone, anyone can claim to be anyone else, including a bank officer, FBI agent, or police officer. A pleasant voice claiming to be from the "Credit Card Protection Bureau" is certainly a scammer if he or she asks you for your credit card numbers and their expiration dates.

Don't go overboard on this, of course. If you initiate the call to a legitimate company that has a telephone order desk, it's safe to provide the order-taker with your credit card number. Be careful only if you're not the one initiating the call. Some telescammers make seemingly irresistible offers to people on the telephone for the sole purpose of obtaining their credit card numbers and expiration dates. Don't buy anything with your credit card on the telephone if you're not the one who initiated the call. Better believe it!

Shred Personal Papers

Don't throw bank account documents, old checks, credit statements, etc., into the garbage. Remember there are "dumpster divers" who can recover your financial statements and use them for theft of your identity.

What do you do with old checkbook pads? You may have used up all the checks, but do you just throw away any unused deposit slips? If so, remember that these too have your address and checking account

number, and this is as good as a check to an identity thief. All he has to do is to file a change of address order with the post office and send for more checks in your name. He'll then be able to write "paper" on your checking account.

Also, shred any "pre-approved" credit card applications, as these too can provide lots of useful information to dumpster divers. If in doubt, shred it.

Buy and use a shredder. A strip shredder is very inexpensive, and some sell for ten or twenty dollars at chain drugstores. A "cross-cut" shredder is much more secure than a strip shredder because it turns papers into confetti. However, a cross-cut shredder is also somewhat more expensive and less reliable. Today a shredder is becoming as much of a fixture in American homes as a TV or stereo. Shredders, like digital cameras, are increasing in quality and reliability and their prices keep dropping. Most importantly, shredders are far less expensive than falling victim to dumpster divers and their accomplices.

Never Fill Out "Consumer Surveys"

You may receive a thick envelope containing a questionnaire from a marketing company. The ostensible purpose of the questionnaire is to discover your preferences and tastes so that companies can make the products you like.

At best, this is a trick to generate tightly focused mailing lists for junk mail. The result will be that you'll receive more junk mail than before. At worst,

it's to discover personal information about you that an identity theft artist can use to steal your identity.

Of course, if you have a little time to spare, and want to expend a first class stamp to make life harder for junk mailers, fill out the questionnaire using a totally fake name and address. Make up your "facts" as you go along, positioning your imaginary character in an upper income bracket so that marketers will conclude that he has a lot of disposable income. Your first class stamp will cause a junk mailer to spend many times that before the returned mailings show him that the survey you filled out is bogus.

Don't "Trust Your Instincts"

The cliché, "trust your instincts," has been around for years, copied by many writers in many different contexts, and has been offered as protection from menaces such as fraud, rape, and serial murder. It's very bad advice, because a con artist is skilled at lulling his victims into complacency and a feeling of safety. Confidence men are called that because they know how to build a victim's confidence, obtaining the victim's trust so that they can scam him.

Let's digress for a paragraph to consider the tactics of one of the most successful serial killers in American history, Ted Bundy. Bundy's victims weren't stupid or especially credulous. However, they were vulnerable to someone of Bundy's expertise.

Bundy was good-looking and projected a sense of vulnerability through carefully planned tactics. He

asked his victims to help him carry bags or bundles, and made sure he always appeared polite and clean-cut. In one case, he wore a cast on his arm to appear helpless and handicapped, using this to defeat his victim's cautious attitudes. They "trusted their instincts," and this led them to their doom.

You can be sure that a con artist who tries to defraud you will appear respectable, and will do everything he can to gain your confidence. He'll dress neatly, be good-looking, shake your hand with a firm grip, and look you in the eye when he speaks. Salesmen, both honest and dishonest, know that the first step in making a sale is to get the buyer to like them: "You have to sell yourself before you can sell the product."

In some cases his position will inspire trust. As we've seen, some doctors are unethical, and they defraud their patients or the health insurance plan in various ways. Your doctor may try to razzle-dazzle you with medical jargon to persuade you to undergo unnecessary treatments, or he may bill your health insurer for treatments he does not deliver. Given this handicap, how do you protect yourself against these skilled deceivers?

Instead of going by "instinct," go by what you've learned of the ways con artists operate, and watch for behavioral cues. This means that you'll be able to articulate your reasons for being distrustful, instead of relying on a vague feeling of instinct. For example, if the scammer's offer appears too good to be true, and he tries to hurry you, these are two excellent, easily defined reasons for being very careful.

However likeable the con artist may be, certain of his tactics should appear like red flags to you. An unwillingness to provide a written contract or an address for his business, using technical jargon that's hard to follow, and an effort to rush you into buying are all danger signals. If you have any doubt about the validity of the offer, take time out to think, and lay out your reasons for doubt in your own mind.

Keep Aware of Your Finances

Keep a mental checklist of when your bills and financial statements are due. This is especially true of credit card bills, because often they're the first indication you have that someone is piggybacking on your account. Always scrutinize your credit card statement for charges you did not run up, and notify the company immediately if there's a charge you don't remember. If you're convinced that someone has made fraudulent use of your credit card number, you can have it cancelled immediately.

Be especially watchful if one month your monthly statement does not appear. Credit card con artists often file fake changes of addresses with credit card providers. This is to divert their victims' statements to postpone the moment when the victim becomes aware that someone's running up fraudulent charges on his card. If you have a curbside mailbox it's very easy for a fraud artist to drive by and snatch your mail, then file a change of address on any accounts he intends to purloin.

Also be careful if you've applied for a credit card and it doesn't arrive. Check with the credit card provider. If it's been mailed to you, chances are that a mail thief has snatched it from your mailbox. Of course, if all of your mail stops arriving, check with your local post office.

You can disregard one piece of advice given by some security specialists: Send for a credit report on yourself every year. Supposedly this will reveal if someone has set up fake credit card accounts in your name. This is in reality almost useless, because of the interval involved. A fraud artist can have set up dozens of fake accounts and milked your actual accounts dry by the time the thefts show up on a credit report.

Safeguard Your Mail

If you live in an older house and receive mail through a slot in your door, you're relatively safe. Likewise if your mail comes to a locked curbside mail station, with individual boxes for each residence. Both are less vulnerable than an ordinary curbside tin mailbox with a hinged end. The key word here is "relatively." All mailboxes are vulnerable, even the official blue post office collection boxes outside your local post office.

Remember that both your incoming and outgoing mail are open to theft. If you write a check, place it in an envelope, and leave it in your insecure curbside mailbox, a thief can drive by, flip down the lid, and steal your envelope. Checks and other valuable per-

sonal documents sent to you can suffer the same fate. This can become very serious with the plethora of unsolicited credit card applications sent out by greedy credit card providers. They're already filled in with your name and address, and a scam artist just has to add a few details, sign your name, and he receives a credit card in your name. Of course, he'll file a change of address, so that the new account statements don't show up in your box.

The traditional ways of delivering mail are insecure in the face of the new wave of criminals. Mail thefts are too common to allow any complacency these days. The USPS Web site offers a clue regarding why. It advises citizens to file a form (PS Form 2016) with the Postal Inspectors if they see a mail theft. It goes on to say:

"By analyzing information collected from this form, Postal Inspectors may determine whether your problem is isolated or part of a larger mail theft problem in your neighborhood — and it may help inspectors locate and apprehend the thieves."

In other words, calling the Postal Inspectors may help catch the perpetrators. Postal Inspectors will not rush to a mailbox theft. With only about 2,000 inspectors for the entire country, and most of them tied up working child porn cases, they don't have much time left to protect the U.S. Postal Service's mailboxes.

If you're to protect your mail, you have to adopt other tactics, not necessarily the ones advocated by the U.S. Postal Service. An example of bad advice gleaned from the U.S. Postal Service's Web site is

this: "Never send cash in the mail. Use checks or money orders."

This is stupid advice, for the same reason discussed above in the paragraphs on credit cards. Of course you don't want to lose cash, but it's even worse if a thief obtains one of your checks. With this, he'll have your account number and will be able to vacuum-clean your checking account before you know it. Although it's more time-consuming to obtain, a money order is much less risky because the most you stand to lose is the amount of the money order, not the balance in your checking account. If you report the loss of the money order promptly, you may be able to recover the money, but at best this will take a long time.

Take care when writing checks. Some mailbox thieves use a chemical solution to bleach the ink from a check, then make it out for a larger amount. Use a "gel" pen to defeat this. A gel pen's ink stays in the paper, and will not wash off. A typical gel pen is the Sanford Uni-Ball Gel RT. There are other brands of gel pens, and they come in different colors.

Now let's look at how to safeguard your outgoing mail. Don't leave anything valuable in a curbside mailbox, or even in a "security" mailbox in your housing complex. Bring it to the post office, and preferably drop it into a mail slot inside the post office building. Many post offices have curbside collection boxes, and these offer good security, but only during daylight hours. Today, it's good practice not to deposit mail after the last collection of the day, because the boxes can be broken into during the night.

Now let's look at incoming mail. Make it your business to pick up your mail promptly, and don't leave it in the curbside box for several hours. If you're away at work during the day, you're out of luck, unless you have a good neighbor who will keep an eye out for your mail and pick it up promptly.

If you go away on vacation, file an "Authorization to Hold Mail," Form 8076, with your local post office. Likewise if you move. Be sure to file a change of address form with your local post office and notify your important correspondents early, before you make your move. As you can understand, incoming mail gathering in your mailbox is a liability.

If your mail stops showing up, contact your local post office immediately to find out if someone's filed a change of address form in your name. The key word here is "immediately." Quick action can help Postal Inspectors locate the fraud artist when he receives your re-directed mail.

More important is to close any accounts that may have been compromised. If you find that your mail's been diverted, or that someone has stolen outgoing mail from your curbside mailbox, don't wait for bogus checks to start appearing. Remember that prevention is better than taking action after you've been robbed. Add the total of outstanding checks that have not yet cleared. Then go immediately to your bank and transfer the surplus to a new account. This keeps a check forger from looting all of your funds.

It's also good practice to keep only a small operating balance in your checking account. Checking accounts

draw very little interest, and the balance is exposed to theft. As a rule of thumb, keep only enough money on hand in your checking account to pay one or two months' bills. Keep the rest in other accounts.

Consider renting a U.S. Postal Service mailbox inside a post office building. This keeps your mail in a safe place until you pick it up, and the chances of your incoming mail being purloined are tiny. The inconvenience is that you'll have to go pick up your mail instead of having it delivered. Also, you'll have to pay a modest rental fee. This is an expense, but so are the locks on your doors, the bars on your windows, your alarm system, your safe, shredder, and any other security devices you have.

A better way is to rent a mail box from a private mail receiving service, often called a "mail drop." The post office will hate you for it, but you're better off with a private service for several reasons. The official U.S. Postal Service post office accepts only U.S. mail, and will not accept any deliveries from United Parcel Service, Federal Express, or other private carriers. A private mail drop accepts UPS, Fedex, and any other delivery addressed to you.

One drawback to private mail drops is that the post office discriminates against their clients. The post office will not accept a change of address form if you have a private mail drop, and you'll have to notify each of your correspondents individually if you move. However, this works in your favor if you receive a lot of junk mail, as most of it will not follow you to your new address.

You may not receive mail every day, but you cannot telephone the post office to find out if there's any mail waiting in your box. The post office is an arm of the government, and they don't have to do anything they don't want to. Private services will gladly tell you if anything has come in for you, because service is part of their business.

Many older post offices shut up tightly after office hours. The more modern ones have lobbies accessible after business hours, to allow mailbox customers access. The modern mail drops, especially the chains and franchises with names such as "Mail 'N More" and "Mail Boxes Etc." have this as a standard feature. You don't have to rush from work to pick up your mail, but can do it any time with a lobby key. The latest "Mail Boxes Etc." stores give each customer a proximity card to operate the door lock after hours without a key. You just hold your proximity card in front of an electronic box to unlock the door.

Private mail drops also offer an array of other services that the post office is now slowly copying to try to remain competitive. Private mail drops sell stamps, envelopes, packing materials, copy machine service, send and receive faxes and e-mails, and provide other services to their customers.

Safeguard Your Computer

We've seen that some programs offered as downloads are actually scams. If you encounter one of these, you can get an early warning by carefully read-

ing the "user agreement." This lays out the conditions of use, something that many subscribers don't bother reading.

There are other ways to protect yourself. Don't download programs you don't know. Don't allow your children to get on the Internet without your supervision, as some of these scammers (and others) prey on children.

The variety of malicious programs sent out on the Internet grows every day. These are of various types, such as "worms," "viruses," etc. Some are designed to destroy data on your computer. Others are designed to scan your computer and retrieve the data on it, and send it to a recipient. Yet others are designed to replicate themselves and send copies out to everyone on your e-mail address list. Finally, some are relatively harmless, just practical jokes that place a funny message on your screen. Many are disguised as attachments to e-mail messages. Once you open the attachment, the malicious program infects your computer.

Spam is a plague for some Internet users. Some spam is merely to induce you to buy something. Other spam messages are fraudulent. In any case, if you find your e-mail inbox flooded with spam, take a few steps to reduce the amount of spam you receive.

A basic step that doesn't cost you anything is to avoid posting messages on bulletin boards and discussion groups. Many spammers obtain an address list by scanning discussion groups, and if you leave your e-mail address on one or more, you can expect to receive spam.

If you must communicate via these discussion groups, set up a separate mailbox with a free private service, such as "Hotmail" or "Yahoo." That way, any spam your posts generate will not go to your regular e-mail address. You may periodically clear out your alternate e-mail address, or if the volume becomes too great, abandon it altogether.

There is another trick that some use to avoid getting spam. This is to insert extra letters into your e-mail address when you post a message. Instead of johnsmith@aol.com, write johnNOSPAMsmith@aol.com. This will keep a spammer who uses a program to sweep the posts for e-mail addresses from getting a useful address. Anything he sends you will come back to him as "undeliverable." Meanwhile, you can insert a sentence into your post saying that if anyone wants to write you, to remove the "NOSPAM" from the address.

Finally, never buy anything from a spammer, because spammers work the same way as junk mailers. If you respond to spam, this just puts you on a special list and you'll receive more spam than before.

Consider signing up for a cable modem service, and disconnect your computer from the telephone line. This will absolutely prevent any stealth feature from running up astronomical telephone bills in your name.

Another advantage of a cable modem is that the amount of spam you receive will drop sharply. Dial-up services seem to provide happy hunting grounds for spammers, but cable modem operators have very effective spam filters in their facilities. Cable modem

services are expensive compared to those that provide dial-up service, but "you get what you pay for."

While we're on the topic of your computer, take a few simple steps to safeguard the information on your computer. Do not use your hard drive for any sensitive information, such as financial records, bank account numbers, etc. Keep these on a separate disk that you can store separately in a safe place. That way, if someone breaks in and steals your computer, all they'll get is the hardware. Don't give them your bank accounts as a bonus.

There's another reason for storing sensitive information on separate disks. If your computer has an Internet connection, there are "Trojan Horse" programs that can scan your hard drive for information and send it to another computer connected to the Internet. Some fraud artists use this stratagem to obtain sensitive information without the victim's knowledge. The "Trojan Horse" can scan only information that is physically in your computer. If you keep sensitive information on a separate disk, it's out of reach. Of course, make sure that you remove any such disks when you log on to the Internet.

As an extra security precaution, if you have two computers, use one for Internet contacts and the other for storing and processing sensitive financial information. The reason is that Internet scammers are becoming increasingly sophisticated. There's a risk that a Trojan Horse program may lie dormant in your computer until you insert a floppy disk, whereupon it will scan that disk, copy the information from it, and squirt it to the scammer the next time you log on to

the Net. Only a totally separate computer can prevent this type of clandestine program from infecting it and stealing your information.

Be careful of information you find on the Internet. Don't buy anything if your sole source of information about it is spam. Many Internet investment fraud artists use spam. Also be extremely careful of any information you pick up in financial chat rooms and bulletin boards. Some posts may be genuine, but in reality it's hard to tell.

Joe Ruffini, a noted information and computer security expert, says, "You don't know what you don't know." You don't know who posted that message on a bulletin board, so you have no way of knowing if the information is valid. Likewise, don't enter into any deal with someone who remains anonymous. You don't know whom that person might be, so always ask for identity verification before you even consider a deal. Obtain a name, not a "handle," ask for an address and a phone number. Then check him out, and make sure he's valid.

One way, not always reliable, is to call the Better Business Bureau. The problem with the BBB is that many of the sellers are in far away places, and the local BBB is unlikely to provide information about them. Another major problem with the Better Business Bureau is that fraudulent businesses relocate often, get new telephone numbers, and it's hard to keep track of them. By the time complaints begin piling up, the information is obsolete. "You cannot assume that an absence of complaints means the offer is legiti-

mate," says Bob Whitelaw, President of the Canadian Council of Better Business Bureaus.[9]

Government sources are also limited. Although the Department of Justice, the Secret Service, and the FBI are involved in tracking down and prosecuting scam artists, none of these maintain lists of legitimate and fraudulent telemarketers or other sellers. In short, you're often on your own.

Be especially careful if the person is using a free e-mail service. Fraud artists know that it's hardest to trace them through such a free service, because they can log on using any name they wish, and nobody will check them out before setting up the free e-mail account.

Charitable Contributions

We've seen that many "charities" are outright scams, and that even "legitimate" charities are not all they seem because not all of your money goes to the ostensible purpose. Some "legitimate" charities are cooking their books so flagrantly that they've been the subjects of a Congressional investigation. What, then, can you do if you want to use some of your spare cash to help people?

First, forget about tax deductions. If your purpose is to help people, don't worry about whether you can deduct the contribution on your income tax form. Charities had lobbied Congress to obtain tax-deductible status to induce people to give more freely. It's only a gimmick.

If you really want to help people with your spare income, consider direct help. Run your own private charity. There are people at work or near where you live who are facing hard times. Consider mailing them cash anonymously, in a tightly sealed envelope.

Another way to do it is to scan your local newspaper for listings of needy people. Some newspapers run articles on needy families just before Christmas, and urge readers to donate directly to them. Unlike conventional charities, these newspapers absorb the overhead, and do not deduct anything for expenses. One contributor contacted the newspaper and accompanied the mother of a needy family on a shopping trip to buy essentials for her children.

Finally, small local charities run only by volunteers are another choice. A local organization is more responsible, and it does not have the multi-million dollar overheads that large national organizations have.

Missing Checks or Cards

If worse comes to worst, and you lose your wallet, or your home gets burglarized, or your mail is stolen, there are a couple of steps to take immediately. Speed is important, because these thieves act quickly to make their fraudulent purchases before the victim can react.

Notify police immediately, but only if you have reason to believe that they can apprehend the perpetrator immediately. If you have seen the thief drive away in a vehicle and you've copied the number, this infor-

mation can help police to run him down within minutes, given a little luck. On the other hand, if the break-in took place hours ago, and there are no witnesses, or if you lost your wallet hours ago, notifying police no longer has the same urgency. By all means call the cops, but there are a couple of high priority actions you must carry out immediately.

First, if your checks or material relating to your checking or other bank account have been stolen, call your bank immediately. Keep your bank's 24-hour number handy, just in case.

If your credit cards are missing, call the credit card issuers immediately to have the cards deactivated. Copy the toll-free numbers off your cards and keep them in your notebook, keep a copy in your desk, and yet another copy in a suitcase if you're traveling. Copying the numbers takes only a few minutes, but can save you hours of grief.

Finally, call the three major credit reporting companies to place a "fraud alert" on your cards. This will prevent a thief from opening a new account in your name, using the information on your credit cards. The toll-free numbers for the three major credit bureaus are:

Equifax:	(800) 525-6285
Experian:	(800) 301-7195
Trans Union:	(800) 680-7289

Also be aware that the Social Security Administration has a fraud reporting number, and this will be important to you if you're on Social Security and your check has been stolen. The number is: (800) 269-0271.

After you've taken care of these high-priority items, call the police. The reason is to generate a police report to substantiate your claim of having been burglarized. If you're lucky enough to live in a locale where the police come to your home or office to investigate a burglary, ask the officer for the case number and a copy of the police report. Be aware, though, that in many areas police no longer come to take burglary reports. You'll get shunted to a clerk who will take your report over the phone. Make sure to ask for a case number, and ask how you may obtain a copy of the police report. Remember that government organizations are often slow, and you may not receive a copy right away. You might be able to speed up the process by offering to come to pick up a copy of the report. There may be a fee involved, perhaps a dollar or two for each page.

If you intend to make a claim to your insurance company, a copy of the police report is essential, because the police report substantiates your claim of having been victimized. This is why you should stop at a copy shop on the way home and make at least a dozen copies. You'll need one for your insurance company, bank, credit card providers, and others.

On a larger scale, what can you do? We've seen how and why the police are not very effective, and why lack of international cooperation hampers enforcement. Let's look next at possible ways to improve the picture.

Notes

1. *Beware of Unexpected Charges for Buyers Clubs*, Press Release, National Consumers League, July 25, 2000.
2. Rayburn, Rosalie, "Taking 'No' For An Answer," *Albuquerque Journal,* Business Outlook, October 4, 2001, p. 1.
3. Rayburn, Rosalie, "Qwest Customers Say Wireless Trial Offer Is Misleading," *Albuquerque Journal,* Business Outlook, October 4, 2001, p. 7.
4. Smith, Brendan, "Pair Sues MCI Over Message," *Albuquerque Journal*, September 27, 2001, p. A1.
5. *Ibid.*
6. www.guidestar.com/news/features/direct_mail.htm
7. www.state.ma.us/consumer/new/beforeyougive.htm
8. Daniels, Dave, Certified Communications Security Professional, *Credit Card and Identity Fraud Scams*, p. 1.
9. http://www.bbb.org/alerts/sweepstakes.asp

Chapter Eleven
Possible Remedies

As we've seen, fraud in the new century is pervasive and profitable. Because of the tremendous amounts of money fraud artists can gain with little risk, fraud has become international in scope.

Fraud used to be a cottage industry in the "good old days" before we were born. Individual practitioners built reputations based on their ingenuity and guile. Today, the picture has reversed, and fraud is often an international enterprise. By contrast, the police agencies to which most people turn for help are the cottage industries, because of their limited jurisdictions.

What, therefore, are the possible steps we can use to cope effectively with fraud artists? The key word in this question is "effectively," because lazy and incompetent legislators and other politicians are fond of "feel-good" laws, to make the citizens feel better under the illusion that the problems are under control. Ineffective laws aren't worth the paper on which they're

printed, and most legislative paper's only real use is in the toilet.

Likewise, laws not effectively enforced are worthless. There's no point in passing severe legislation if the perpetrators remain out of reach in other states or countries. Similarly, the best laws are useless if the police don't have the will, the means, or the support to enforce the laws.

As an example of the difficulties involved in multi-agency efforts, consider the Puget Sound area, which has experienced a large increase in mail and identity thefts during the last couple of years. A corresponding increase in meth lab busts has also occurred. Why has the problem become so severe?

The King County, Washington area is not exactly devoid of law enforcement officers. Among the agencies cooperating on the twin problems are the U.S. and Washington Attorney's Offices, the Postal Inspection Service, the King County Sheriff's Drug Enforcement Unit, the Washington Department of Social and Health Services, etc. However, a King County detective stated that it's going to take more than meetings.[1]

Meanwhile, the thefts continue to increase. This is typical of what happens when fragmented American law enforcement agencies try to cooperate. High-level officials hold meetings, and produce letters of understanding and delegations of responsibilities, etc. These are mere bureaucratic maneuvers that don't accomplish much but look good in the headlines. In severe instances, legislators may get into the act and in-

troduce "feel-good" laws that address the problem but don't contribute to its solution.

Federal Law Enforcement

The U.S. Department of Justice, the FBI, the U.S. Secret Service, and other federal agencies have staff assigned to the fraud problem. These try to run down fraud artists with varying degrees of effectiveness. Let's look at a couple of operations the Department of Justice ran during the 1990s and see how effective they were.

The Department of Justice announced "Operation Disconnect" on March 4, 1993. The FBI did the grunt work during this undercover operation, pretending to sell a machine that would enable telescammers to dial 12,000 calls an hour. As they pretended to be explaining the operation of the machine to telemarketers, FBI agents working undercover asked them many questions about their operations, on the pretext that this information was necessary to tailor the machine to their use. By this means, FBI agents obtained many damaging admissions for use in prosecutions. The net result was that the Department of Justice was able to prosecute 700 scammers, some receiving sentences as high as 10 years in prison.[2]

Another undercover FBI operation was "Senior Sentinel," disclosed on December 7, 1995. Federal agents took over the telephones of people who had reported having been victimized multiple times, possibly because the telescammers kept records of vulnerable

people, and posed as the victims. Recording the conversations, they developed evidence of use in prosecutions. The result was that about 1,000 crooked telemarketers suffered prosecution, and some received prison sentences as high as 14 years.[3]

The Department of Justice Web site does not provide a follow-up to these cases because the information provided is designed to put the Department of Justice in the best possible light. There is no discussion of how many convicted telescammers had their sentences reduced by parole, or how many won early release because valuable prison space was needed for other prisoners.

Practical experience, however, shows us that despite these investigations and prosecutions during the first half of the 1990s, telefraud has increased. Today, we are bombarded by more telemarketing calls than ever before, and a proportion of them are fraudulent. As we've seen several times in this book, nobody keeps central records of all the fraud cases.

What is clear is that the much-vaunted federal prosecutions didn't put much of a dent in fraud artists' operations. Now that we're in the early part of the 21st century, telefraud is proliferating. Telescammers are agile in ways that outclass conventional law enforcement. They not only relocate quickly to stay ahead of the cops, but they take advantage of opportunities very quickly. As we saw in an earlier chapter, the terrorist attacks of September 11, 2001, resulted in telescammers piggybacking on the devastation to

bilk people of their money and, in certain cases, their identities.

Security Enhancements

Another approach suggested is a technical one. There are many security safeguards in producing identity documents and credit cards that are hard to counterfeit. There are other means, such as digital signatures, biometrics, and authentication. The National Fraud Center has proposed "authentication" as the tool against identity theft. "Authentication" means verifying the identity of a party to a transaction by technical means. However, identity thieves have to date, managed to cope with every countermeasure.

Notes

1. Skolnik, Sam, "Meth Use Linked to Jump in ID, Mail Thefts," *Seattle Post-Intelligencer*, July 23, 2001.
2. http://www.usdoj.gov/criminal/fraud/telemarketing/doj.htm
3. *Ibid.*

Chapter Twelve
Our International Role

As the planet's sole surviving super power, the United States has tremendous leverage to enforce an international program to combat fraud. The United States hands out favors, such as "most favored nation trading status" and various forms of foreign aid. Unfortunately, this country often doesn't use its power. Evidence of this is the faltering "war on drugs," where we let citizens of foreign nations export illegal drugs to the United States. Our various "drug czars" have given a lot of lip service to stopping the growth of illegal crops in foreign countries, and their importation, but have taken no effective action.

We can call for, and pressure other countries to enter into treaties with teeth in them, to bite organized criminals hard. The first step is to eliminate sanctuaries for organized fraud artists. This is essential, because many of today's fraud rings know that cooperation between different countries' judicial systems is

half-hearted, at best, and few criminals have to fear extradition.

Canada is a good example. We've seen how many scammers operate north of the border with the confidence that they can get away with it forever. In 1997, law enforcement officials from both countries met to set up a joint effort to combat cross-border fraud. They set up several operations and made a number of recommendations to fight fraud. The Bi-National Telemarketing Fraud Group formed a part of the Canada-U.S. Cross-Border Crime Forum. The RCMP set up Project Colt in the eastern part of the country, and Project Emptor in Vancouver, British Columbia. Now, years after the agreement, we can evaluate the results. We still have telemarketing fraud, and it's stronger than ever. Let's look at a couple of reasons why:

One recommendation adopted was Bill C-20, which among other things provides for denying telephone service to criminal organizations that have been convicted. While this looks good on paper, in practice it's essential to apprehend and convict a criminal telemarketer to deny him service. Because they're fast moving, they're hard to catch. Even after conviction, they can set up shop under another name and obtain telephone service. Other recommendations are vaguely worded, feel-good provisions that are basically ineffective.

Treaties can also set up international task forces to combat multi-national fraud rings. This will give the phrase "the long arm of the law" real meaning. Teams

of experienced investigators authorized to operate across national boundaries can carry the investigations wherever they lead and apprehend the perpetrators.

A uniform penal code is also important, to ensure that fraud artists will not escape penalties by operating from a country with "slap on the wrist" sanctions. A severe difficulty is that many countries have laws prohibiting crimes within their borders, but using the country as a base for crimes in other countries is legal. As an example, practically every country has laws prohibiting the counterfeiting of its currency, but few ban the faking of other countries' money.

We see the same with long-distance telephone and Internet scams. Fraud rings operating across national boundaries are relatively safe, because they live in one country but defraud victims in another. Their country of residence does not have jurisdiction in the countries where the victims live, and law enforcement officials in the victims' home states or countries do not have jurisdiction where the criminals have their base.

One type of international treaty that is a step in the right direction is the Convention on Cybercrime, drafted by the European Committee on Crime Problems. This treaty would allow law enforcement to cross national boundaries, either virtually or physically, in pursuit of cyber-criminals. However, some self-styled "privacy advocates" have objected to the proposed treaty's ratification, claiming that it allows law enforcement too much latitude.[1]

More severe penalties for chronic offenders may help. It's important to think of medical fraud artists

as organized criminals, and to treat them the same way. In some countries, such as China, organized criminals receive the death penalty for economic crimes, and their organs are harvested for transplants. In the West, we're squeamish about putting people to death for non-violent crimes, but it's still possible to cope with these offenders. Long prison sentences are one answer. To be effective, sentences must be real, not merely nominal figures degraded by parole, probation, or early release programs.

Large fines must be part of the picture. We've seen that many frauds are carried out by "legitimate" corporations, and letting them know that criminal penalties will hit them in the bottom line will be effective. Right now, the worst that often happens is that a lower-level executive takes the blame, while top officers claim innocence and escape penalties. Multimillion dollar fines will make an impression that won't be forgotten, especially when they have an impact on executive bonuses.

Notes

1. Piazza, Peter, "Cybercrime Treaty Opens Pandora's Box," *Security Management*, Volume 45, Number 9, September 2001, p. 40.

Resources

Although you, personally, are the first line of defense against fraud, you can't fight the problems alone. Apart from recognizing the warning signs of fraud and not allowing yourself to be a victim, reporting frauds to law enforcement agencies can help. Unfortunately, many law enforcement agencies are not geared to fighting fraud, and it's important to pick the right one. Be prepared to get a run-around, as many agencies simply don't know how to handle fraud cases. This is why you should record the numbers of several agencies that might be concerned, and telephone more than one.

It's usually not appropriate to call 911 for a non-emergency, such as reporting a fraud. Most police agencies have a non-emergency number. Look up the number of your local agency and write it here:

_____

Your state attorney general may have a special fraud division and it may be worth contacting this office. Look up this number and write it here: _____

A list of state attorneys general is available at the web site: http://www.naag.org/about/aglist.cfm

The FBI also gets involved in certain types of frauds as well as other federal crimes. Write the number of the FBI's local field office here: _____

The FBI main number in Washington, DC, is: 202-324-3000.

The U.S. Postal Service's Postal Inspectors have jurisdiction over identity thefts involving the mail. Look up the number of the nearest Postal Inspector and write it here_____

The U.S. Secret Service handles computer crimes and identity theft, among other crimes, so look up the number of the nearest field office and write it here: _____

Social Security Administration Fraud Hot Line: 800-269-0271

Equifax
PO Box 105873
Atlanta, GA 39348-5873
Phone: 800-997-2493
Fraud line: 800-525-6285
Web site: www.equifax.com

Experian Information Solutions (formerly TRW)
PO Box 949
Allen, TX 75013-0949
Phone: 888-397-3742
Fraud Line: 800-301-7195
Web site: www.experian.com

Trans Union
PO Box 930
Springfield, PA 19064-0390
Phone: 800-916-8800
Fraud line: 800-680-7289
Web site: www.tuc.com

Better Business Bureau

The Better Business Bureau offers information about some frauds, and some companies that have had judgments against them. The national web site also offers information regarding whether a particular business is a member of the BBB. There are specific web pages devoted to some fraudulent practices.

The BBB's web site is: http://www.bbb.org/

U.S. Department of Justice

The U.S. Department of Justice has a fraud section, and several operations aimed at frauds. For example, Operation Disconnect and Operation Senior Sentinel resulted in federal criminal charges against more than 1,300 telescammers.
http://www.usdoj.gov/criminal/fraud/telemarketing/doj.htm

However, we must be realistic. Telemarketing fraud artists are still out there. Federal prosecution doesn't appear to have cramped their style. Federal prosecutors can ask for severe penalties, such as five years' imprisonment, but only if the scammers are caught. You can get some information at the DOJ Web site: http://www.usdoj.gov/

To report specific frauds, call the FBI. Web site: www.fbi.gov

Federal Trade Commission

The Federal Trade Commission serves to regulate trade and to fight economic crimes. Among its projects are a section devoted to identity theft. The FTC maintains a regularly updated Web site on identity theft: Web site: http://www.consumer.gov/idtheft

Federal Trade Commission Fraud Line: 877-IDTHEFT (877-438-4338)

The FTC also answers questions and accepts complaints regarding consumer fraud, including telemarketing fraud.

Federal Trade Commission Consumer Response Center:
877-382-4357
202-326-3128

Calling these numbers may help. At least, it will get the information into the pipeline and distributed to law enforcement agencies. Obviously, if a large number of complaints come in about a particular fraud scheme, there's more likely to be an effort made than if only one or two complaints arrive.

Global Fraud Alert

Global Fraud Alert is an advisory group formed by computer industry personnel to collect and disseminate information on frauds. Based in Australia and other Far East countries, Global Fraud Alert is one of a very few information networks that is truly international in coverage, as are many fraud artists.

GFA operates a Web site to provide information on varieties of frauds committed in many countries and across national boundaries.

Global Fraud Alert
Level 50, 101 Collins Street
Melbourne, 3000, Australia
Phone: +613 96539647
Web site: www.globalfraudalert.com

GuideStar

GuideStar bills itself as "The National Database of Nonprofit Organizations." Its database contains listings for more than 850,000 such groups, and a quick search feature that allows finding an organization with a keyword or title. The entries provide a quick profile of the organization, including its name, address, and financial picture.

Web site: www.guidestar.com/

Healthcare Corporate Compliance Supersite

HC Complianceinfo.com is the "Healthcare Corporate Compliance Supersite." This Web site maintains information on compliance with health care regulations, mainly for the benefit of HMOs, hospitals, nursing care facilities, doctors, and other health care prac-

titioners. In reality, many problems are the result of ignorance or mistakes in billing, and this site provides information regarding federal and state regulations and how to comply with them. The practical reason is that the paperwork involved in billing can be bewildering, and a mistake can result in an investigation in the same way that a deliberate fraud can.

For the typical health care consumer, this site also provides information on legal actions, including criminal prosecutions of doctors and institutions that fall on the wrong side of the law.

A subsection titled "Entire News Archive" provides names and dates of regulatory and criminal actions relating to fraud and possible fraud. A weekly newsletter, *Compliance Monitor*, provides accounts of the latest events that often do not appear in the regular news media. The address is:
HCPro
200 Hoods Lane
Marblehead, MA 01945
Phone: 800-650-6787
Fax: 781-639-7857
Web site: www.complianceinfo.com

National Consumers League

National Consumers League is a consumer advocacy organization that warns consumers about frauds and other items of interest. Web site: www.ncinet.org

National Fraud Information Center

National Fraud Information Center is operated by Trans Union Corp, one of the big three credit reporting bureaus. Its purpose is to spread information about the latest trends in frauds among the financial services, the insurance industry, consumers, and the casino industries.
Phone: 800-876-7060
Web site: www.fraud.org/welmes.htm

U.S. Postal Inspection Service

The Postal Inspectors provide information about postal frauds, and you can file a complaint with them. The Web site also has a checklist of how to check out a charity with which you're unfamiliar. Web site: www.usps.gov/depart/inspect

U.S. Secret Service

The U.S. Secret Service is one of the best of the federal law enforcement agencies, and has a Financial Crimes Division. The Secret Service originally had the job of combating counterfeiting of money. More recently it was assigned to protect the U.S. President and other government officials. Another area of responsibility is combating certain types of fraud, such as the Nigerian scams and computer fraud. The address is:
950 H Street, NW
Washington, DC 20001
Phone: 202-406-5850
Fax: 202-406-5031

Web site: www.treas.gov/usss
E-mail: 419.fed@usss.treas.gov

U.S. Securities and Exchange Commission

The SEC provides information about securities frauds. You can also file a complaint if you think you've been defrauded. The site has a wealth of information to use in checking out any company offering stock. The home page has a heading, "Regulatory Action," and this provides a listing of actions taken against individuals and companies. Check this out before investing. Another heading, "Litigation," covers trading suspensions, administrative proceedings, and other actions taken against people and companies in the financial world.

Web site: www.sec.gov

Verizon

Verizon Phone Fraud Alliance is a Web site operated by this wireless provider to document the latest telephone fraud scams, from identity-theft related cons to holiday scams. Members of the Phone Fraud Alliance include several telephone companies, such as Pacific Bell, Southwestern Bell, etc. Verizon makes the information available to consumers and regularly updates the Web site.

www.bellatlantic.com/security/fraud/index.htm

YOU WILL ALSO WANT TO READ:

☐ **40091 21st CENTURY FRAUD, How To Protect Yourself in the New Millennium, *by Tony Lesce.*** Fraud artists are very imaginative and creative, with agile minds that adapt to the changing scene around them. This book highlights the need for you to be especially vigilant and to help you develop a paranoid attitude. No one can guarantee you 100% protection, but *21st Century Fraud* is a start. ***2000, 5½ x 8½, 160 pp, soft cover.* $15.95.**

☐ **19197 STREET SMARTS FOR THE NEW MILLENNIUM, *by Jack Luger.*** Life can be risky for the average citizen. There are criminal elements in our society, which pose real dangers to the safety and security of ourselves and our families. In this unique book, author Jack Luger has provided the methods and resources that enable the reader to minimize these threats to our lives, liberties, and pursuit of happiness. You'll learn to: depend on personal resources instead of police; protect yourself, your family and your assets; and earn untraceable income. ***1996, 5½ x 8½, 138 pp, soft cover.* $15.00.**

☐ **58136 COPS! Media vs. Reality, *by Tony Lesce.*** Police officers are ever-popular subjects in the media. Each year brings a new crop of cop movies from Hollywood. Each year we see more crime novels, often written by people with an incomplete knowledge of their subject. They know how to construct a plot, but lack much of the basic knowledge to make their works factually accurate. However, news reporting and documentaries are supposed to be straight facts. Often they're not, because both unconscious bias and editorial choices affect their accuracy. There are many differences in the way law enforcement appears in the media, and the way it really is. This book will explore the reasons why, and present a picture of the way law enforcement really operates. It will highlight the contrasts between the way cops are portrayed on TV and in the movies, and the way they work in real life. ***2000, 5½ x 8½, 145 pp, soft cover.* $13.95.**

MFCG

LOOMPANICS UNLIMITED
PO BOX 1197
PORT TOWNSEND, WA 98368

Please send me the books I have checked above. I am enclosing $ _____ which includes $5.95 for shipping and handling of orders up to $25.00. Add $1.00 for each additional $25.00 ordered. *Washington residents please include 8.2% for sales tax.*

NAME _____

ADDRESS _____

CITY/STATE/ZIP _____

We accept Visa, Discover, and MasterCard. To place a credit card order *only,* call 1-800-380-2230, 24 hours a day, 7 days a week.
Check out our Web site: www.loompanics.com

Modern Frauds and Con Games

by Tony Lesce

Fraud is the fastest growing industry in the world, which is why it's become a global trillion-dollar problem. The main reason is that it's low-risk compared to other crimes. Overall, the apprehension rate is about three percent and the conviction rate is about one percent.

The simple fact is that new and menacing techniques of fraud spring up almost every day.

This volume describes dozens of frauds, many of which are not even illegal, but do involve deception for economic gain. This book will shed light on the new frauds and con games, with an extensive chapter on steps you can take to reduce your vulnerability to fraud. No book on fraud can be the final word, but this will help you protect yourself and your family.

Chapters include: • Medical Fraud • Internet Fraud • Identity Theft • Charity Frauds • Airline Security Scams • Possible Remedies • and much, much more.

Get Modern Frauds and Con Games and start protecting yourself today.

$15.00

ISBN 1-55950-224-X

EAN 9 781559 502245 90000

W7-DCT-769